

(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
19 March 2009 (19.03.2009)

PCT

(10) International Publication Number
WO 2009/036183 A1(51) International Patent Classification:
G07F 7/10 (2006.01) H04L 29/08 (2006.01)
G06K 19/00 (2006.01)(74) Agents: COX, Michael E. et al.; Fish & Richardson P.C.,
P.O. Box 1022, Minneapolis, Minnesota 55440-1022 (US).(21) International Application Number:
PCT/US2008/076033(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA,
CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE,
EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID,
IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK,
LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW,
MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT,
RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ,
TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM,
ZW.(22) International Filing Date:
11 September 2008 (11.09.2008)(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL,
NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG,
CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).(25) Filing Language: English
(26) Publication Language: English
(30) Priority Data:
60/971,813 12 September 2007 (12.09.2007) US
12/205,821 5 September 2008 (05.09.2008) US**Published:**

- with international search report
- before the expiration of the time limit for amending the
claims and to be republished in the event of receipt of
amendments

(54) Title: SELECTIVELY SWITCHING ANTENNAS OF TRANSACTION CARDS

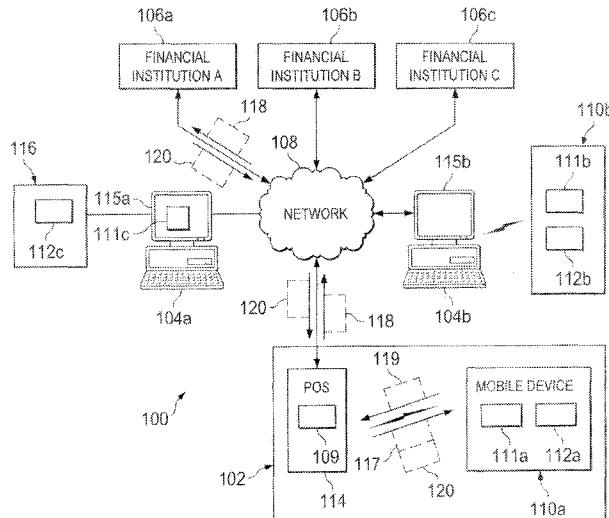


FIG. 1

WO 2009/036183 A1

(57) Abstract: The present disclosure is directed to a system and method for selectively switching antennas of transaction cards. In some implementations, a method includes physically interfacing a card with a mobile host device including a Graphical User Interface (GUI). The card executes wireless financial transactions independent of the mobile host device. User credentials used to execute financial transactions with retail terminals are stored. Information is presented through the GUI of the mobile host device. An antenna of the card is selectively switched between an activate state and an inactive state in response to at least an event.

Selectively Switching Antennas of Transaction Cards

CLAIM OF PRIORITY

This application claims priority to U.S. Patent Application Serial No. 60/971,813, filed on September 12, 2007, and U.S. Patent Application Serial No. 5 12/205,821, filed on September 5, 2008, the entire contents of which are hereby incorporated by reference.

TECHNICAL FIELD

This invention relates to network communications and, more particularly, to wirelessly executing financial transactions.

10

BACKGROUND

Portable electronic devices and tokens have become an integrated part of the regular day to day user experience. There is a wide variety of common portable and handheld devices that users have in their possession including communication, business and entertaining devices such as cell phones, music players, digital cameras, 15 smart cards, memory token and variety of possible combinations of the aforementioned devices and tokens. All of these devices share the commonality that consumer are accustomed to carrying them with them most of the time and to most places. This is true across the various demographics and age groups regardless of the level of the sophistication of the consumer, their age group, their technical level or 20 background.

These common handheld devices offer options for expandable memory. Micro Secure Digital (microSD) is the popular interface across high-end cellphones while SD and MultiMediaCard (MMC) interfaces are also available in limited models. MicroSD is the least common denominator supported by the majority of these devices and tokens (in terms of size). In addition, adaptors are available to convert a MicroSD into 25 MiniSD, SD, MMC and USB. Although most popular MP3 player (iPOD) offer's a proprietary interface, competing designs do offer standard interfaces. Digital cameras offer mostly SD and MMC while extreme Digital (xD) is another option. Micro and Mini versions of these interfaces are also available in several models. Mini-USB is

increasingly available across cellphones, digital cameras and MP3 players for synchronization with laptops.

SUMMARY

The present disclosure is directed to a system and method for selectively switching antennas of transaction cards. In some implementations, a method includes physically interfacing a card with a mobile host device including a Graphical User Interface (GUI). The card executes wireless financial transactions independent of the mobile host device. User credentials used to execute financial transactions with retail terminals are stored. Information is presented through the GUI of the mobile host device. An antenna of the card is selectively switched between an activate state and an inactive state in response to at least an event.

The details of one or more embodiments of the invention are set forth in the accompanying drawings and the description below. Other features, objects, and advantages of the invention will be apparent from the description and drawings, and 15 from the claims.

DESCRIPTION OF DRAWINGS

FIGURE 1 is an example transaction system in accordance with some implementations of the present disclosure;

FIGURE 2 is an example transactions system that transmits transaction 20 information through a cellular core network;

FIGURE 3 is an example transaction card of FIGURE 1 in accordance with some implementations of the present disclosure;

FIGURE 4 is an example intelligent card that selectively switching an antenna;

FIGURE 5 is an example secure memory of an intelligent card for storing 25 multiple user credentials;

FIGURE 6 is a schematic diagram illustrating personalization processes of intelligent cards;

FIGURES 7A and 7B are flow charts illustrating an example method for initialize an intelligent card;

30 FIGURES 8A, 8B and 8C are examples of call flow illustrating call sessions with an intelligent card;

FIGURE 9 is a flow chart illustrating an example method for activating a transaction card; and

FIGURES 10A and 10B illustrate example cards for housing intelligent cards. Like reference symbols in the various drawings indicate like elements.

5

DETAILED DESCRIPTION

FIGURE 1 is a block diagram illustrating an example transaction system 100 for wirelessly executing transactions using an intelligent card independent of a host device. For example, the system 100 may include a microSecure Digital (microSD) card that executes transactions with financial institutions independent of a host device.

10 Aside from microSD, the system 100 may include other mass storage interfaces that connect an intelligent card to the host device such as, for example, MultiMediaCard (MMC), SD, Universal Serial Bus (USB), Apple iDock, Firewire, and/or others. An intelligent card is a device configured to insert into or otherwise attach to a host device and access or otherwise execute services (e.g., transactions) independent of the host

15 device. In some implementations, the intelligent card may be shaped as a microSD card including, for example, notches, raised portions and/or other features. The system 100 may include an intelligent card that includes a dual interface. The dual interface may connect the intelligent card to both the host device through a physical interface (e.g., SD, MMC, USB) and external devices through a wireless connection (e.g., NFC, ISO 14443). In some implementations, the intelligent card may include an embedded

20 secure chip, Central Processing Unit (CPU) with operating system, local memory and value added applications accessible by the user through the host device. A host device may include a cellphone, a smartphone, a Personal Digital Assistant (PDA), a MPEG-1 Audio Layer 3 (MP3) device, a digital camera, a camcorder, a client, a computer,

25 and/or other device that includes a mass memory and/or peripheral interface. In some implementations, the intelligent card can operate as a master with the host device being a slave such that the intelligent card controls operational aspects of the host device such as a user interface. The intelligent card in the system 100 may execute one or more of the following: selectively activate an antenna for wireless transactions

30 in response to at least an event; verify the host device with a financial institution through, for example, a Point Of Sale (POS) using a host signature; execute a transaction with a financial institution through, for example, a POS terminal

independent of the host device; and/or other processes. By providing an intelligent card, the system 100 may wirelessly execute transactions with financial institutions without either requiring additional hardware, software, and/or firmware on the host device and/or without requiring changes to existing hardware, software, and/or 5 firmware for reader terminals to enable a user to wirelessly execute a transaction.

At a high level, the system 100 includes an offline store 102 and clients 104a and 104b coupled to financial institutions 106 through a network 108. While not illustrated, the system 100 may include several intermediary parties between the financial institution 106 and the network such as, for example, a transaction acquirer 10 and/or a payment network host. The offline store 102 includes a mobile device 110a having a transaction card 112a and a Point of Sale (POS) device 114 that executes transactions with customers. The POS device 114 includes a Graphical User Interface (GUI) 109 for presenting information to and/or receiving information from users. In some implementations, the POS 114 may transmit a request to execute a transaction to 15 the transaction card 112. The transaction card 112 may transmit authentication information to the POS 114. The client 104 includes the GUI 115 for presenting information associated with the system 100. The client 104a includes a card reader 116 that interfaces the transaction card 112c with the client 104a. The financial institution 106 may authorize the transaction based, at least in part, on information 20 transmitted by the transaction card 112. The mobile device 110 includes a GUI 111 for presenting information associated with financial transactions.

The offline store 102 is generally at least a portion of an enterprise having a physical presence (e.g., building) for operations. For example, the offline store 102 may sell goods and/or services at a physical location (e.g., a brick-and-mortar store) 25 directly to customers. In this example, the offline store 102 buys or otherwise receives goods (e.g., produce) from distributors (not illustrated) and then may sell these goods to customers, such as users of the mobile device 110. In general, the offline store 102 may offer face-to-face experiences with customers in providing goods and/or services. For example, the offline store 102 may be a click-and-mortar store such that a user 30 selects a good or service using the Internet and purchases and receives the good or service at the offline store 102. The offline store 102 may provide one or more of the following services associated with goods: inventory, warehousing, distribution, and/or transportation. As a result, the offline store 102 may not immediately distribute goods

received from distributors. The offline store 102 may include a single retail facility, one or more retail facilities at a single geographic location, and/or a plurality of retail facilities geographically distributed. In some cases, two or more entities may represent portions of the same legal entity or affiliates. For example, the offline store 102 and 5 distributors may be departments within one enterprise. In summary, the offline store 102 may wirelessly execute financial transactions with the mobile device 110.

Each mobile device 110 comprises an electronic device operable to interface with the transaction card 112a. For example, the mobile device 110 may receive and transmit wireless and/or contactless communication with the system 100. As used in 10 this disclosure, the mobile devices 110 are intended to encompass cellular phones, data phones, pagers, portable computers, SIP phones, smart phones, personal data assistants (PDAs), digital cameras, MP3 players, camcorders, one or more processors within these or other devices, or any other suitable processing devices capable of communicating information with the transaction card 112. In some implementations, 15 the mobile devices 110 may be based on a cellular radio technology. For example, the mobile device 110 may be a PDA operable to wirelessly connect with an external or unsecured network. In another example, the mobile device 110 may comprise a smartphone that includes an input device, such as a keypad, touch screen, mouse, or other device that can accept information, and an output device that conveys 20 information associated with a transaction with the offline store 102, including digital data, visual information, or GUI 111.

The GUI 111 comprises a graphical user interface operable to allow the user of the mobile device 110 to interface with at least a portion of the system 100 for any suitable purpose, such as authorizing transactions and/or displaying transaction history. 25 Generally, the GUI 111 provides the particular user with an efficient and user-friendly presentation of data provided by or communicated within the system 100 and/or also an efficient and user-friendly means for the user to self-manage settings and access services offered by the financial institution 106. The GUI 111 may comprise a plurality of customizable frames or views having interactive fields, pull-down lists, 30 and/or buttons operated by the user. The term graphical user interface may be used in the singular or in the plural to describe one or more graphical user interfaces and each of the displays of a particular graphical user interface. The GUI 111 can include any

graphical user interface, such as a generic web browser or touch screen, that processes information in the system 100 and presents the results to the user.

The transaction card 112 can include any software, hardware, and/or firmware configured to wirelessly execute transactions with the POS device 114. For example, 5 the transaction card 112 may execute a contactless transaction with the POS device 114 independent of the mobile device 110a. In other words, the transaction card 112 may wirelessly execute transactions without aspects of the transaction being executed by the mobile device 110. The transaction card 112 may execute transactions with the POS device 114 using short range signals such as NFC (e.g., ISO 18092/ECMA 340), 10 ISO 14443 type A/B, ISO 15693, Felica, MiFARE, Bluetooth, Ultra-wideband (UWB), Radio Frequency Identifier (RFID), contactless signals, proximity signals, and/or other signals compatible with retail payment terminals (e.g., POS 114). In some implementations, the transaction card 112 may include one or more chipsets that execute an operating system and security processes to independently execute the 15 transaction. In doing so, the mobile device 110 does not require additional hardware, software, and/or firmware to wirelessly execution a transaction with the POS 114 such as an NFC transaction. In some implementations, the transaction card 112 may execute one or more of the following: wirelessly receive a request from the POS device 114 to execute a transaction and/or and provide a response; translate between 20 wireless protocols and protocols compatible with the transaction card 112; translate between transaction-card protocols and protocols compatible with mobile device 110; present and receive information (e.g., PIN request, PIN) from the user through the GUI 111; decrypt and encrypt information wirelessly transmitted between the transaction card 112 and the POS 114; execute applications locally stored in the transaction card 25 112; selectively switch the antenna of the transaction card 112 on and off based, at least in part, on one or more events; execute authentication processes based, at least in part, on information received, for example, through the GUI 111; transmit a host signature to POS 114 in response to at least a transaction challenge; store, at least in part, details of the transaction executed between place between the card 112 and the 30 POS device 114; generate and/or present alerts (e.g., audio-visual alerts) to the user through the GUI 111; generate and/or transmit wireless-message alerts to the financial institution 106 using the mobile device 110 if cellular capable; and/or others. In some implementations, the transaction card 112 may include a communication module with

of a protocol translation module, antenna tuning circuit, power circuit and a miniature antenna tuned to exchange wireless data with a retail terminal 114.

In some implementations, the transaction card 112 may initiate a transaction in response to at least a user selecting a graphical element in the GUI 111. The 5 transaction card 112 may initiate a transaction with the POS 114 in response to at least wireless request transmitted by the POS 114. In some implementations, the transaction card 112 may selectively switch the antenna between an on and off state in response to one or more events. The one or more events may include a user request, completion of 10 transaction, insertion of card 112 in a different mobile device, location change, timer events, detection of incorrect PIN entered by the user, change of wireless network that the device is connected to, message received from the financial institution 106 using wireless communication methods such as SMS, and/or other events. For example, the transaction card 112 may receive one or more commands to switch the antenna off from a cellular network (not illustrated) through the mobile device 110. In some 15 implementations, the transaction card 112 may request user identification such as a PIN, a user ID and password combination, biometric signature, and/or others.

In regards to translating between protocols, the transaction card 112 may process information in, for example, ISO 7816, a standard security protocol, and/or others. In this case, the transaction card 112 may translate between an NFC protocol 20 (e.g., ISO 18092) and the transaction-card protocol. In some implementations, ISO 7816 commands may be encapsulated within interface commands used to transmit data between the host device 114 and the card 112. In addition, the transaction card 112 may interface the mobile device 110 through a physical interface such as MicroSD, Mini-SD SD, MMC, miniMMC, microMMC, USB, miniUSB, microUSB, firewire, 25 Apple iDock, and/or others. In regard to security processes, the transaction card 112 may implement one or more encryption algorithms to secure transaction information such as card number (e.g., credit card number, debit-card number, bank account number), PIN, and/or other security related information. The security related information may include an expiry date, card verification code, user name, home 30 phone number, user zip code and/or other user information associated with verifying an identity of the card holder. In some implementations, the transaction card 112 may execute private key (symmetric algorithms) such as DES, TDES and/or others or public key (asymmetric algorithms) such as RSA, elliptic curves, and/or others. In

addition, the transaction card 112 may include memory (e.g., Flash, EEPROM) for storing user data, applications, offline Webpages, and/or other information. In regards to applications, the transaction card 112 may execute a locally stored application and present information to and received information from the user through the GUI 111.

5 For example, the transaction card 112 may execute an application used to synchronize an account balance with the financial institution 106 using the GUI 111 and the mobile device 110. Alternatively or in addition to applications, the transaction card 112 may present offline Web pages to the user using the GUI 111. In response to initiating a

10 transaction, the transaction card 112 may automatically present an offline Web page through the GUI 111. In some implementations, the offline Web page can be associated with a financial institution 106. In some implementations, the transaction card 112 can be backward compatible and operate as a mass storage device. For example, if the wireless interface of the transaction card 112 is not available or deactivated, the transaction card 112 may operate as a mass storage device enabling users to access

15 data stored in the memory component (e.g., Flash). In some implementations, the transaction card 112 can execute a set of initialization commands in response to at least insertion into the mobile device 110. These initialization commands may include determining device related information for the mobile device 100 (e.g., phone number, signature, connected network information, location information and other available properties), determining user relating information (e.g., PIN code, activation code), incrementing counters, setting flags and activating/deactivating functions according to

20 pre-existing rules and/or algorithms.

In some implementations, the transaction card 112 may automatically execute one or more fraud control processes. For example, the transaction card 112 may

25 identify an operational change and automatically transmit a notification to the financial institution based, at least in part, on the identified change. The transaction card 112 may execute two fraud control processes: (1) determine a violation of one or more rules; and (2) automatically execute one or more actions in response to at least the violation. In regards to rules, the transaction card 112 may locally store rules

30 associated with updates to operational aspects of the transaction card 112. For example, the transaction card 112 may store a rule indicating a change in mobile host device 110 is an operational violation. In some implementations, the transaction card 112 may store rules based, at least in part, on updates to one or more of the following:

phone number of host device 110; MAC address of host device 110; network wirelessly connected to host device 110; location of host device; and/or other aspects. In response to one or more events matching or otherwise violating rules, the transaction card 112 may execute one or more processes to substantially prevent or 5 otherwise notify the financial institutions 106 of potentially fraudulent activity. For example, the transaction card 112 may execute a command to block an associated user account and/or the transaction card 112. Alternatively or in addition, the transaction card 112 may transmit a command to the financial institution 106 to call the mobile host device 110. In some implementations, the transaction card 112 may execute a 10 command based, at least in part, on an event type. In some examples, the transaction card 112 may initiate a call with the financial institution 106 in response to at least a change in number of the host device 110. In some examples, the transaction card 112 may re-execute an activation process in response to at least a specified event type. An activation process may include activating the transaction card and/or financial account 15 as discussed in more detail with respect to FIGURE 9. In some implementations, the transaction card 112 may execute a command to disconnect the GUI 111 from the transaction card 112. The transaction card 112 may present a disconnection notification through the GUI 111 prior to executing the command. In some implementations, the transaction card 112 may transmit a command to the financial 20 institution 106 to deactivate an account associated with the card 112.

In some implementations, the POS 114 may transmit a transaction request 117 to the transaction card 112 for information to generate an authorization request 118. In response to at least the transaction request, the transaction card 112 may transmit one or more transaction responses 119 identifying information associated with a payment 25 account. In some implementations, the POS device 114 may transmit a request 118 to authorize a transaction to the financial institution 106. The authorization information may include an account number, a transaction amount, user credentials, and/or other information. In response to at least the transaction request 118, the financial institution 106 may transmit an authorization response 120 to the POS device 114. In some 30 implementations, the POS device 114 may transmit the response 120 to the transaction card 112. The transaction response 120 may include, for example, a receipt presentable to the user through the GUI 111a. In some implementations, the financial institution 106 may transmit the authorization response 120 to the mobile device

through a cellular core network (see FIGURE 2). In this implementation, the financial institution 106 may have stored the association between the mobile device 110 and the transaction card 112 during the user sign-up process, automatically upon user activation of the card 112 when, for example, the card 112 is initially inserted into the 5 mobile device 110, and/or other event. In the illustrated implementation, the POS 114 includes the GUI 109.

The GUI 109 comprises a graphical user interface operable to allow the user of the POS 114 to interface with at least a portion of the system 100 for any suitable purpose, such as a user entering transaction information (e.g., PIN, transaction 10 acceptance) and/or and presenting transaction information (e.g., transaction amount). Generally, the GUI 109 provides the particular user with an efficient and user-friendly presentation of data provided by or communicated within the system 100 and/or also an efficient and user-friendly means for the user to initiate a wirelessly transaction with the transaction card 112. The GUI 109 may present a series of screens or displays 15 to the user to, for example, accept a transaction and enter security information such as a PIN.

In some implementations, the transaction card 112 can be implemented differently. The transaction card 112 may be implemented as a KeyFOB and remains live outside the mobile device 110 as a FOB. In this case, the transaction card 112 20 may be passive and powered from an induction magnetic field generated by the POS 114. The transaction card 112 may be implemented in the form of an industrial integrated circuit chip for mounting on a PCB or IC chip. In some implementations, the transaction card 112 may be implemented in the form of a self contained desktop standalone unit powered by external AC adapter or stand alone box. In some 25 implementations, the transaction card 112 can be implemented as an external attachment to a mobile device 110 (e.g., case) and connected to the mobile device using a peripheral interface such as USB, serial port, the iDock apple proprietary interface, and/or other interface.

In some implementations, the transaction card 112 may operate in accordance 30 with one or more of the following modes: active card emulation; active reader; self train; killed; memory; inactive; and/or other modes. The transaction card 112 may operate active-card-emulation mode to convert the mobile device 110 to a contactless payment device loaded with a financial vehicle (FV) that may be, for example, a credit

card, a debit card, a gift card and/or other retail payment product. In this mode, the transaction card 112 may execute payment transactions at any capable retail payment terminal (e.g., POS 114) that accepts contactless payment transactions. For example, such terminals may be contactless-enabled terminals currently being deployed by 5 merchants under MasterCard's paypass, Visa's paywave programs, Amex ExpressPay, Discover Zip, and/or other payment programs. After the antenna of the transaction card 112 is activated in this mode, a merchant terminal may detect the presence of a host device with the transaction card 112 and prompt the user to authorize a transaction such as by entering a PIN, signing on a terminal interface, confirming the amount of 10 the transaction, and/or other action. In this mode, such transactions may be handled as a normal card-present transaction. In other words, the POS 114 may perceive the transaction card 112 as a contactless plastic payment card and may communicate with the transaction card 112 as a contactless plastic payment card to execute payment transactions. In these implementations when the card 112 operates in an active-card 15 emulation mode, the POS 114 can wirelessly communicate with the transaction card 112 using the same signals used to communicate with a contactless plastic payment card. In this active-card emulation mode, the transaction card 112 emulates a contactless plastic payment card and may be backward compatible with the POS 114. In this implementation, neither the terminal nor the financial institution may require 20 additional software to execute the transaction. In addition, the transaction card 112 in this mode may be used for other applications such as physical access control (to open gates either in a corporate environment or in a transit environment), logical access control (to request network access via a PC), application access control (to buy access for amenities such as transportation, movies or wherever payment needs to be made to 25 gain access to a facility), and/or other applications.

In the active-reader mode, the transaction card 112 may convert the mobile device 110 to a contactless reader device capable of receiving data when in range of a transmitting terminal (e.g., POS 114). In some implementations, this mode can require special NFC hardware with reader mode capability as part of the transaction card 112. 30 In the event that the mobile device 110 is proximate (e.g., 10 cm or less) a transmitting terminal, the reader mode of the transaction card 112 may activated and prompt the user for authorization to receive data through the GUI 111. This mode may only be suitable for mobile devices 110 with a UI element, such as an OK button and a screen,

an LED to indicate that data reception is being requested, and/or other interfaces. Once the user authorizes the transmission, the transaction card 112 in this mode may receive, and locally store, process and may execute a transaction and/or forward received data to another entity. For example, the transaction card 112 in this mode may receive 5 content through promotional posters, validating the purchase of a ticket, and/or others. For example, the transaction card 112 in this mode may function as a mobile POS terminal receiving transaction information from a plastic contactless card/FOB and instructing the POS 114 to prepare a transaction authorization request for the financial institution 106 through a cellular core network. Once the financial institution 106 10 authorizes the transaction, the mobile device 110 may display the confirmation of the transaction to the user through the GUI 111.

In regards to the self-train mode, the transaction card 112 may execute a version of the reader mode. In some implementations, the self-train mode can be activated by a special action (e.g., a needle point press to a small switch, entry of an 15 administrative password via the GUI 111). In response to at least activating this mode, the transaction card 112 may be configured to receive personalization data over, for example, the short range wireless interface from another peer transaction card such as the plastic contactless cards compliant with this functionality and issued by the financial institution 106 or a specially prepared administrative card for this purpose. 20 Personalization data received in this mode may include encrypted FV information that is stored in secured memory of the transaction card 112. In some implementations, the transaction card 112 in this mode may receive the FV information through a contactless interface of a transmitter and/or others. The transaction card 112 may then synthesize the FV information that corresponds to the user account and personalize an 25 internal security module that includes, for example, payment applications for executing transactions with financial institutions 106 and associated user credentials. The self-train mode may be used to re-personalize the transaction card 112 in the field. In some implementations, all previous data can be deleted if the self-train mode is activated. The self-train mode may be a peer-to-peer personalization mode where the 30 card 112 may receive personalization information from another transaction card 112. This mode may represent an additional personalization mode as compared with factory, store and/or Over-The-Air (OTA) personalization scenarios which may be server to client personalization scenarios. In some implementations, the self-train

mode may be a peer-to-peer personalization mode where the transaction card 112 receives personalization information from another transaction card. Since two transaction cards 112 are used in this mode, this mode may be different from a server-to-client personalization scenario as with a factory, store, and OTA personalization.

5 In regards to the inactive mode, the transaction card 112 may temporarily deactivate the contactless interface. In some implementations, the inactive mode can be activated through the physical interface with the mobile device 110 such as a microSD interface. In response to at least the activation of the inactive mode, the transaction card 112 may temporarily behave as only a mass-memory card. In some 10 implementations, the card 112 may also enter this state when the reset needle point is pressed. In this mode, the transaction card 112 may preserve locally-stored information including financial user data. In this mode, the transaction card 112 may execute the activation process and if successful may return to the active mode. Financial institutions 106 may use this mode to temporarily prevent usage in response 15 to at least identifying at least potentially fraudulent activity.

In regards to the killed mode, the transaction card 112 may permanently deactivate the contactless interface. In some implementations, the killed mode is activated through the physical interface with the mobile device 110 such as a microSD interface. In response to at least the activation of the killed mode, the transaction card 20 112 may permanently behaves as a mass memory stick. In the event that the reset needle point is pressed, the transaction card 112 may, in some implementations, not be made to enter any other modes. In addition, the transaction card 112 may delete financial content in memory in response to at least this mode being activated. In some implementations, financial institutions 106 may use this mode to delete data from a 25 transaction card 112 that is physically lost but still connected to the wireless network via the host device 110.

In regards to the memory mode, the transaction card 112 may operate as a mass memory stick such that the memory is accessible through conventional methods. In some implementations, the transaction card 112 may automatically activate this mode 30 in response to at least being removed from the host device, inserted into a non-authorized host device, and/or other events. The transaction card 112 may be switched to active mode from the memory mode by, for example, inserting the card 112 into an authorized device or may be switched from this mode into the self-train

mode to re-personalize the device for a new host device or a new user account. In some implementations, the memory mode may operate substantially same as the inactive mode.

In some implementations, the transaction card 112 may be re-personalized/updated such as using software device management process and/or a hardware reset. For example, the user may want to re-personalize the transaction card 112 to change host devices, to have multiple host devices, and/or other reasons. In regards to the software device management, the user may need to cradle the new host device with the transaction card 112 inserted to launch the software device management application. In some implementations, the software management application can be an application directly installed on the client 104, integrated as a plug-in to a normal synchronization application such as ActiveSync, available via a browser plug-in running on the plug-in provider's website, and/or other sources. The user may log into the application and verify their identity, and in response to verification, the application may allow access to a devices section in the device management application. The device management application may read the transaction card 112 and display the MAC addresses, signatures of the devices that he has inserted his plug-in to, and/or other device specific information. The mobile device 110 may be marked as active and the host device may be shown as disallowed or inactive. The application may enable the user to update the status of the new host device, and in response to at least the selection, the device management application may install the signature on the new host device and mark update the status as allowable in secure memory of the transaction card 112. The user may be able to also update the status of the mobile device 110 to disallowed. Otherwise, both devices may be active and the transaction card 112 may be switched between the two devices. In regards to the hardware reset process, the user may use the reset needle point press on the physical transaction card 112 to activate the self-train mode. In this mode, the financial data may be deleted and have to be reloaded. When the transaction card 112 is inserted into the new host device, the provisioning process may begin as discussed above.

The POS 114 can include any software, hardware, and/or firmware that receives from the transaction card 112 account information for executing a transaction with one or more financial institutions 106. For example, the POS 114 may be an

electronic cash register capable of wirelessly communicating transaction information with the transaction card 112a. The POS 114 may communicate transaction information associated with traditional contact payment methods such as plastic cards and checks. If enabled for wireless/contactless payment transactions, the POS 114 5 may communicate information with the transaction card 112 in one or more the following formats: 14443 Type A/B, Felica, MiFare, ISO 18092, ISO 15693; and/or others. The transaction information may include verification information, check number, routing number, account number, transaction amount, time, driver's license number, merchant ID, merchant parameters, credit-card number, debit-card number, 10 digital signature and/or other information. In some implementations, the transaction information may be encrypted. In illustrated implementation, the POS 114 can wirelessly receive encrypted transaction information from the transaction card 112 and electronically send the information to one or more of the financial institutions 106 for authorization. For example, the POS 114 may receive an indication that a transaction 15 amount has been accepted or declined for the identified account and/or request additional information from the transaction card 112.

As used in this disclosure, the client 104 are intended to encompass a personal computer, touch screen terminal, workstation, network computer, a desktop, kiosk, wireless data port, smart phone, PDA, one or more processors within these or other 20 devices, or any other suitable processing or electronic device used for viewing transaction information associated with the transaction card 112. For example, the client 104 may be a PDA operable to wirelessly connect with an external or unsecured network. In another example, the client 104 may comprise a laptop that includes an input device, such as a keypad, touch screen, mouse, or other device that can accept 25 information, and an output device that conveys information associated with transactions executed with the financial institutions 106, including digital data, visual information, or GUI 115. In some implementations, the client 104b can wirelessly communicate with the transaction card 112b using, for example, an NFC protocol. In some implementations, the client 104a includes a card reader 116 having a physical 30 interface for communicating with the transaction card 112c. In some implementations, the card reader 116 may at least include an adapter 116b that adapts the interface supported by the client 104 (e.g., USB, Firewire, Bluetooth, WiFi) to the physical

interface supported by the card 112 (e.g., SD/NFC). In this case, the client 104a may not include a transceiver for wireless communication.

The GUI 115 comprises a graphical user interface operable to allow the user of the client 104 to interface with at least a portion of the system 100 for any suitable purpose, such as viewing transaction information. Generally, the GUI 115 provides the particular user with an efficient and user-friendly presentation of data provided by or communicated within the system 100. The GUI 115 may comprise a plurality of customizable frames or views having interactive fields, pull-down lists, and/or buttons operated by the user. The term graphical user interface may be used in the singular or in the plural to describe one or more graphical user interfaces and each of the displays of a particular graphical user interface. The GUI 115 can include any graphical user interface, such as a generic web browser or touch screen, that processes information in the system 100 and presents the results to the user. The financial institutions 106 can accept data from the client 104 using, for example, the web browser (e.g., Microsoft Internet Explorer or Mozilla Firefox) and return the appropriate responses (e.g., HTML or XML) to the browser using the network 108. In some implementations, the GUI 111c of the transaction card 112c may be presented through the GUI 115a of the client 104a. In these implementations, the GUI 115a may retrieve user credentials from the GUI 111c and populate financial forms presented in the GUI 115a. For example, the GUI 115a may present a forum to the user for entering credit card information to purchase a good through the Internet, and the GUI 115a may populate the form using the GUI 111c in response to at least a request from the user.

Financial institutions 106a-c can include any enterprise that may authorize transactions received through the network 108. For example, the financial institution 106a may be a credit card provider that determines whether to authorize a transaction based, at least in part, on information received through the network 106. The financial institution 106 may be a credit card provider, a bank, an association (e.g., VISA), a retail merchant (e.g., Target), a prepaid / gift card provider, an internet bank, and/or others. In general, the financial institution 106 may execute one or more of the following: receive a request to authorize a transaction; identify an account number and other transaction information (e.g., PIN); identify funds and/or a credit limit associated with the identified account; determine whether the transaction request exceeds the funds and/or credit limit and/or violates any other rules associated with the account;

transmit an indication whether the transaction has been accepted or declined; and/or other processes. In regards to banking, the financial institution 106 may identify an account number (e.g., bank account, debit-card number) and associated verification information (e.g., PIN, zip code) and determine funds available to the account holder.

5 Based, at least in part, on the identified funds, the financial institution 106 may either accept or reject the requested transaction or request additional information. As for encryption, the financial institution 106 may use a public key algorithm such as RSA or elliptic curves and/or private key algorithms such as TDES to encrypt and decrypt data.

10 Network 108 facilitates wireless or wired communication between the financial institutions and any other local or remote computer, such as clients 104 and the POS device 114. Network 108 may be all or a portion of an enterprise or secured network. While illustrated as single network, network 108 may be a continuous network logically divided into various sub-nets or virtual networks without departing from the 15 scope of this disclosure, so long as at least a portion of network 108 may facilitate communications of transaction information between the financial institutions 106, the clients 104, and the offline store 102. In some implementations, network 108 encompasses any internal or external network, networks, sub-network, or combination thereof operable to facilitate communications between various computing components 20 in system 100. Network 108 may communicate, for example, Internet Protocol (IP) packets, Frame Relay frames, Asynchronous Transfer Mode (ATM) cells, voice, video, data, and other suitable information between network addresses. Network 108 may include one or more local area networks (LANs), radio access networks (RANs), metropolitan area networks (MANs), wide area networks (WANs), all or a portion of 25 the global computer network known as the Internet, and/or any other communication system or systems at one or more locations.

FIGURE 2 is a block diagram illustrating an example transaction system 200 for wirelessly communicating transactions information using cellular radio technology. For example, the system 200 may wirelessly communicate a transaction receipt to a 30 transaction card 112 using a mobile host device 110 and cellular radio technology. In some implementations, cellular radio technology may include Global System for Mobile Communication (GSM), Code Division Multiple Access (CDMA), Universal Mobile Telecommunications System (UMTS), and/or any other cellular technology.

The financial institutions 106 may assign one or more mobile host devices 110 to a transaction card 112 in response to one or more events. In some examples, the user may register the one or more mobile devices 110 with the financial institution 106 in connection with, for example, requesting the associated transaction card 112. In some 5 examples, the transaction card 112 may register the mobile host device 110 with the financial institution 106 in response to at least an initial insertion into the device 110. Regardless of the association process, the system 100 may use the cellular capabilities of the host devices 110 to communicate information between the financial institutions 106 and the transaction card 112. In using the cellular radio technology of the host 10 device 110, the system 100 may communicate with the transaction card 112 when the card 112 is not proximate a retail device, such as the POS device 114 of FIGURE 1.

In the illustrated implementation, the cellular core network 202 typically includes various switching elements, gateways and service control functions for providing cellular services. The cellular core network 202 often provides these 15 services via a number of cellular access networks (e.g., RAN) and also interfaces the cellular system with other communication systems such as the network 108 via a MSC 206. In accordance with the cellular standards, the cellular core network 202 may include a circuit switched (or voice switching) portion for processing voice calls and a packet switched (or data switching) portion for supporting data transfers such as, for 20 example, e-mail messages and web browsing. The circuit switched portion includes MSC 206 that switches or connects telephone calls between radio access network (RAN) 204 and the network 108 or another network, between cellular core networks or others. In case the core network 202 is a GSM core network, the core network 202 can include a packet-switched portion, also known as General Packet Radio Service 25 (GPRS), including a Serving GPRS Support Node (SGSN) (not illustrated), similar to MSC 206, for serving and tracking communication devices 102, and a Gateway GPRS Support Node (GGSN) (not illustrated) for establishing connections between packet-switched networks and communication devices 110. The SGSN may also contain subscriber data useful for establishing and handing over call connections. The cellular 30 core network 202 may also include a home location register (HLR) for maintaining "permanent" subscriber data and a visitor location register (VLR) (and/or an SGSN) for "temporarily" maintaining subscriber data retrieved from the HLR and up-to-date information on the location of those communications devices 110 using a wireless

communications method. In addition, the cellular core network 202 may include Authentication, Authorization, and Accounting (AAA) that performs the role of authenticating, authorizing, and accounting for devices 110 operable to access GSM core network 202. While the description of the core network 202 is described with respect to GSM networks, the core network 202 may include other cellular radio technologies such as UMTS, CDMA, and others without departing from the scope of this disclosure.

The RAN 204 provides a radio interface between mobile devices and the cellular core network 202 which may provide real-time voice, data, and multimedia services (e.g., a call) to mobile devices through a macrocell 208. In general, the RAN 204 communicates air frames via radio frequency (RF) links. In particular, the RAN 204 converts between air frames to physical link based messages for transmission through the cellular core network 202. The RAN 204 may implement, for example, one of the following wireless interface standards during transmission: Advanced Mobile Phone Service (AMPS), GSM standards, Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), IS-54 (TDMA), General Packet Radio Service (GPRS), Enhanced Data Rates for Global Evolution (EDGE), or proprietary radio interfaces. Users may subscribe to the RAN 204, for example, to receive cellular telephone service, Global Positioning System (GPS) service, XM radio service, etc.

The RAN 204 may include Base Stations (BS) 210 connected to Base Station Controllers (BSC) 212. BS 210 receives and transmits air frames within a geographic region of RAN 204 (i.e. transmitted by a cellular device 102e) and communicates with other mobile devices 110 connected to the GSM core network 202. Each BSC 212 is associated with one or more BS 210 and controls the associated BS 210. For example, BSC 212 may provide functions such as handover, cell configuration data, control of RF power levels or any other suitable functions for managing radio resource and routing signals to and from BS 210. MSC 206 handles access to BSC 212 and the network 108. MSC 206 may be connected to BSC 212 through a standard interface such as the A-interface. While the elements of RAN 204 are described with respect to GSM networks, the RAN 204 may include other cellular technologies such as UMTS, CDMA, and/or others. In the case of UMTS, the RAN 204 may include Node B and Radio Network Controllers (RNC).

The contactless smart card 214 is a pocket-sized card with embedded integrated circuits that process information. For example, the smart card 214 may wirelessly receive transaction information, process the information using embedded applications and wirelessly transmit a response. The contactless smart card 214 may wirelessly 5 communicate with card readers through RFID induction technology at data rates of 106 to 848 kbit/s. The card 214 may wirelessly communicate with proximate readers between 10cm (e.g., ISO/IEC 14443) to 50cm (e.g., ISO 15693). The contactless smart card 214 operates independent of an internal power supply and captures energy 10 from incident radio-frequency interrogation signals to power the embedded electronics. The smart card 214 may be a memory card or microprocessor card. In general, memory cards include only non-volatile memory storage components and may 15 include some specific security logic. Microprocessor cards include volatile memory and microprocessor components. In some implementations, the smart card 214 can have dimensions of normally credit card size (e.g., 85.60 × 53.98 × .76 mm, 5 x 15 x .76 mm). In some implementations, the smart card 214 may be a fob or other security token. The smart card 214 may include a security system with tamper-resistant 20 properties (e.g., a secure cryptoprocessor, secure file system, human-readable features) and/or may be configured to provide security services (e.g., confidentiality of stored information).

20 In some aspects of operation, the financial institution 106 may use the mobile host device 110 to communicate information to the transaction card 112. For example, the financial institution 106 may wirelessly communicate with the mobile host device 110 using the cellular core network 202. In some implementations, the financial institution 106 may transmit information to the mobile host device 110 in response to 25 at least an event. The information may include, for example, transaction information (e.g., transaction receipt, transaction history), scripts, applications, Web pages, and/or other information associated with the financial institutions 106. The event may include completing a transaction, determining a transaction card 112 is outside the operating range of a POS terminal, receiving a request from a user of the mobile host 30 device, and/or others. For example, the financial institution 106 may identify a mobile host device 110 associated with a card 112 that executed a transaction and transmit transaction information to the mobile host device 110 using the cellular core network 202. In using the cellular core network 202, the financial institutions 106 may transmit

information to the transaction card 112 without requiring a POS terminal being proximate to the card 112. In addition or alternatively, the financial institution 106 may request information from the mobile host device 110, the transaction card 112 and/or the user using the cellular core network 202. For example, the financial 5 institution 106 may transmit a request for transaction history to the card 112 through the cellular core network 202 and the mobile host device 110.

In some aspects of operation, a merchant or other entity may operate the mobile host device 110c as a mobile POS terminal configured to wirelessly execute transactions with the smart card 214. For example, a vendor may be mobile (e.g., a 10 taxi driver) and may include a mobile host device 110c with a transaction card 112c. In this example, the transaction card 112c may wirelessly receive account information from the smart card 214 and the POS 114 may transmit an authorization request to the financial institution 106 using the mobile host device 110 and the cellular core network 202. In response to at least the request, the financial institution 106 may generate an 15 authorization response to the transaction card 112c using the mobile host device 110 and the cellular network 202.

In some implementations, the system 100 may execute one or more of the modes discussed with respect to FIGURE 1. For example, the transaction card 112 may be re-personalized/updated using the cellular radio technology of the mobile host 20 device 110. The user may want to re-personalize the transaction card 112 to change host devices, to have multiple host devices, and/or other reasons. In regards to the software device management, the user may transmit to the financial institution 106 a request to re-personalize the transaction card 112 using the cellular radio technology of the host device 110.

25 FIGURE 3 illustrates is a block diagram illustrating an example transaction card 112 of FIGURE 1 in accordance with some implementations of the present disclosure. In general, the transaction card 112 includes personalized modules that execute financial transactions independent of the mobile device 110. The illustrated transaction card 112 is for example purposes only, and the transaction card 112 may 30 include some, all or different modules without departing from the scope of this disclosure.

In some implementations, the transaction card 112 can include an interface layer 302, an API/UI 304, a Web server 306, a real-time framework 308, payment

applications 310, value added applications 312, user credentials 314, real-time OS 316, contactless chipset 318, antenna control functions 320, antenna 322, bank used memory 324, and free memory 326. In some implementations, a host controller includes the interface layer 302, the API/UI 304, the Web server 306, the real-time framework 308, the contactless chipset 318, and the antenna control functions 320. In some implementations, a security module includes the payment applications 310 and the user credentials 314. The bank used memory 324 and free memory 326 may be contained in Flash. In some implementations, the contactless chipset 318 may be integrated within the security module or operated as a standalone. The antenna 322 may be electronic circuitry.

The interface layer 302 includes interfaces to both the host device, *i.e.*, physical connection, and the external world, *i.e.*, wireless/contactless connection. In payment implementations, the wireless connection can be based on any suitable wireless standard such as contactless (*e.g.*, ISO 14443 A/B), proximity (*e.g.*, ISO 15693), NFC (*e.g.*, ISO 18092), and/or others. In some implementations, the wireless connection can use another short range wireless protocol such as Bluetooth, another proprietary interfaces used by retail payment terminals (Felica in Japan, MiFare in Asia, *etc.*), and/or others. In regards to the physical interface, the interface layer 302 may physically interface the mobile device 110 using an SD protocol such as MicroSD, Mini-SD or SD (full-size). In some implementations, the physical interface may include a converter/adapter to convert between two different protocols based, at least in part, on the mobile device 110. In some implementations, the mobile device 110 may communicate using protocols such as USB, MMC, iPhone proprietary interface, or others.

The API/UI layer 304 can include any software, hardware, and/or firmware that operates as an API between the mobile device 110 and the transaction card 112 and as the GUI 111. Prior to executing transactions, the transaction card 112 may automatically install drivers in the mobile device 110 in response to at least insertion. For example, the transaction card 112 may automatically install a MicroSD device driver in the device 110 to enable the transaction card 112 to interface the mobile device 110. In some implementations, the transaction card 112 may install an enhanced device driver such as a Mass Memory with Radio (MMR) API. In this implementation, the interface can drive a class of plug-ins that contain mass memory

as well as a radio interface. The MMR API may execute one or more of the following: connect/disconnect to/from the MMR controller (Microcontroller in the plug-in); transfer data using MM protocol (e.g., SD, MMC, XD, USB, Firewire); send encrypted data to the MMR controller; receive Acknowledgement of Success or Error; received 5 status word indicating description of error; turn radio on/off; send instruction to the transaction card 112 to turn the antenna on with specifying the mode of operation (e.g., sending mode, listening mode); transmit data such as send instruction to controller to transmit data via the radio; listen for data such as send instruction to controller to listen for data; read data such as send instruction to controller to send the data received by 10 the listening radio; and/or others. In some implementations, MMR can be compliant with TCP/IP. In some implementations, API encapsulated ISO 7816 commands may be processed by the security module in addition to other commands.

In some implementations, the API can operate in accordance with the two processes: (1) the transaction card 112 as the master and the mobile device 110 as the 15 slave; and (2) the card UI as the master. In the first process, the transaction card 112 may pass one or more commands to the mobile device 110 in response to, for example, insertion of the transaction card 112 into a slot in the mobile device 110, a transaction between the transaction card 112 and the POS 114, and/or other events. In some implementations, the transaction card 112 can request the mobile device 110 to 20 execute one or more of following functions: Get User Input; Get Signature; Display Data; Send Data; Receive Data; and/or others. The Get User Input command may present a request through the GUI 111 for data from the user. In some implementations, the Get User Input may present a request for multiple data inputs. The data inputs may be any suitable format such as numeric, alphanumeric, and/or 25 other strings of characters. The Get Signature command may request the mobile device 110 to return identification data such as, for example, a phone number, a device ID like an IMEI code or a MAC address, a network code, a subscription ID like the SIM card number, a connection status, location information, Wi-Fi beacons, GPS data, and/or other device specific information. The Display Data command may present a 30 dialog to the user through the GUI 111. In some implementations, the dialog can disappear after a period of time, a user selection, and/or other event. The Send Data command may request the mobile device 110 to transmit packet data using its own connection to the external world (e.g., SMS, cellular, Wi-Fi). The Receive Data

command may request the mobile device 110 to open a connection channel with certain parameters and identify data received through the connection. In some implementations, the command can request the mobile device 110 to forward any data (e.g., SMS) satisfying certain criteria to be forwarded to the transaction card 112.

5 In regards to the UI as master, the UI may execute one or more of the following commands: security module Command/Response; Activate/Deactivate; Flash Memory Read/Write; Send Data with or without encryption; Receive Data with or without decryption; URL Get Data / URL Post Data; and/or others. The security module commands may relate to security functions provided by the card and are directed
10 towards the security module within the transaction card 112 (e.g., standard ISO 7816 command, proprietary commands). In some implementations, the commands may include encryption, authentication, provisioning of data, creation of security domains, update of security domain, update of user credentials after verification of key, and/or others. In some implementations, the commands may include non security related
15 smart card commands such as, for example, read transaction history commands. The read transaction history command may perform a read of the secure memory 324 of the transaction card 112. In some implementations, certain flags or areas of the secure memory 324 may be written to after security verification. The Activate/Deactivate command may activate or deactivate certain functions of the transaction card 112. The
20 Flash Memory Read/Write command may execute a read/write operation on a specified area of the non-secure memory 326. The Send Data with or without encryption command may instruct the transaction card 112 to transmit data using its wireless connection with, for example, the POS 114. In addition, the data may be encrypted by the transaction card 112 prior to transmission using, for example, keys
25 and encryption capability stored within the security module. The Receive Data with or without decryption command may instruct the transaction card 112 to switch to listening mode to receive data from its wireless connection with the terminal/reader (e.g., POS 114). In some implementations, data decryption can be requested by the security module using, for example, keys and decryption algorithms available on the
30 security module, *i.e.*, on-board decryption. The URL Get Data/URL Post Data command may instruct the web server 306 to return pages as per offline get or post instructions using, for example, offline URLs.

The Web server 306, as part of the OS of the transaction card 112, may assign or otherwise associate URL style addressing to certain files stored in the memory 326 (e.g., flash) of the transaction card 112. In some implementations, the Web server 306 locates a file using the URL and returns the file to a browser using standard HTTP, 5 HTTPS style transfer. In some implementations, the definition of the files can be formatted using standard HTML, XHTML, WML and/or XML style languages. The file may include links that point to additional offline storage locations in the memory 326 and/or Internet sites that the mobile device 110 may access. In some implementations, the Web server 306 may support security protocols such as SSL. 10 The Web server 306 may transfer an application in memory 326 to the mobile device 111 for installation and execution. The Web server 306 may request the capabilities of the browser on the device 110 using, for example, the browser user agent profile, in order to customize the offline Web page according to the supported capabilities of the device and the browser, such as, for example, supported markup language, screen size, 15 resolution, colors and such.

As part of the Real time OS, the real-time framework 308 may execute one or more functions based, at least in part, on one or more periods of time. For example, the real-time framework 308 may enable an internal clock available on the CPU to provide timestamps in response to at least requested events. The real-time framework 20 308 may allow certain tasks to be pre-scheduled such that the tasks are executed in response to at least certain time and/or event based triggers. In some implementations, the real-time framework 308 may allow the CPU to insert delays in certain transactions. In some implementation, a part of WAP standards called WTAI (Wireless Telephony Application Interface) can be implemented to allow offline 25 browser pages on the card 112 to make use of functions offered by the mobile device 110 (e.g., send / receive wireless data, send / receive SMS, make a voice call, play a ringtone etc.).

The payment applications 310 can include any software, hardware, and/or firmware that exchanges transaction information with the retail terminal using, in some 30 instances, a pre-defined sequence and/or data format. For example, the payment applications 310 may generate a response to a transaction request by selecting, extracting or otherwise including user credentials in the response, in a format compatible with the retail terminal's payment processing application. In some

implementations, the payment applications 310 may execute one or more of the following: transmit properties of the transaction card 112 in response to at least an identification request received from the POS 114; receive a request to execute a transaction from, for example, the POS 114; identify user credentials in the bank-used memory 324 in response to at least the request; generate a transaction response based, at least in part, on the user credentials; transmit the transaction response to the POS 114 using, for example, a contactless chipset; receive clear data, for example a random number, from the POS 114 and provide a response containing encrypted data by encrypting the clear data using the cryptographic capabilities of the secure element; 5 transmit the encrypted data using the contactless chipset 318; increment a transaction counter with every transaction request received; transmit a value of the transaction counter in response to a request from the POS 114; store details of the transaction request received from the POS 114 into the transaction history area of the bank used memory 324; transmit transaction history to the CPU of the intelligent card 112 in 10 response to such a request; receive ISO 7816 requests from the CPU of the intelligent card 112; execute corresponding transactions using the secure element OS; provide responses back to the CPU; and/or other processes. In generating the transaction response, the payment application 310 may generate the response in a format specified by the payment network (VISA, MasterCard, Amex, Discover) associated with a 15 financial institution 106 or a proprietary format owned and defined by the financial institution 106 and processible by the POS 114. The transaction request may include one or more of the following: user credentials (e.g., account number); expiry data, card verification numbers; a transaction count;; and/or other card or user information. In some implementations, the payment application 310 may comprises a browser 20 application to enable transactions. The browser application 310 may be a browser that may be installed if the device 110 is either missing a browser or has a browser that is incompatible with the Web server 306 on the card 112. After installation of such browser 310, future communications between the mobile device 110 and the web-server 306 make use the newly installed browser.

25 30 The real-time OS 316 may execute or otherwise include one or more of the following: real-time framework 308; a host process that implements the physical interface between the transaction-card CPU and the mobile device 110; an interface that implements the physical interface between the transaction-card CPU and the

security module; a memory-management process that implements the ISO 7816 physical interface between the transaction-card CPU and the memory 324 and/or 326; an application-layer process that implements the API and UI capabilities; the Web server 306; antenna-control functions 320; power management; and/or others. In some 5 implementations, the real-time OS 316 may manage the physical interface between the transaction-card CPU and the secure memory 324 that includes memory segmentation to allow certain memory areas to be restricted access and/or data buffers/pipes. In some implementations, the security module can include a security module OS provided by the security module Vendor and may be compliant with Visa and 10 MasterCard specifications. The security module OS may structure the data in the security module to be compliant with Paypass and/or payWave specifications or any other available contactless retail payment industry specifications. In addition, the security module may store host device signatures and allow modes of the antenna 322 in the secure element 324. In some implementations, the real-time OS 316 may 15 include a microcontroller OS configured to personalizing the secure element 324 such as by, for example, converting raw FV data (account number, expiry date, Card Verification Number (CVN), other application specific details) into secure encrypted information. In addition, the microcontroller OS may present the card 112 as a MicroSD mass storage to the host device. The microcontroller OS may partition the 20 memory into a user section and a protected device application section. In this example, the device application section may be used to store provider specific applications that either operate from this segment of the memory or are installed on the host device from this segment of the memory.

The security module chip may provide tamper-resistant hardware security 25 functions for encryption, authentication, management of user credentials using multiple security domains, on-board processing capabilities for personalization, access and storage, and/or others. In some implementations, the security module chip can include the contactless chipset 318.

The contactless chipset 318 may provides the hardware protocol 30 implementation and/or drivers for RF communication. For example, the contactless chipset 318 may include on-board RF circuitry to interface with an external world connection using a wireless/contactless connection. The wireless connection may be,

for example, client to node (terminal / reader / base station), node to client (passive tag), or peer to peer (another transaction card 112).

The antenna control function 320 may controls the availability of the RF antenna. For example, the antenna control function 320 may activate/deactivate the 5 antenna 322 in response to, for example, successful authentication, completion of a routine established by the OS 316, and/or other event. The antenna 322 may be a short range wireless antenna connected to an NFC inlay via a software switch such as a NAND Gate or other element.

FIGURE 4 is a block diagram illustrating an example intelligent card 400 in 10 accordance with some implementations of the present disclosure. For example, the transaction card of FIGURE 1 may be implemented in accordance with the illustrated intelligent card 400. In general, the intelligent card 400 may independently access services and/or transactions. The intelligent card 400 is for illustration purposes only and may include some, all, or different elements without departing from the scope of 15 the disclosure.

As illustrated, the intelligent card 400 includes an antenna 402, a switch plus tuning circuit 404, a security module and contactless chipset 406, a CPU 408 and memory 410. The antenna 402 wirelessly transmits and receives signals such as NFC signals. In some implementations, the switch plus tuning circuit 404 may dynamically 20 adjust the impedance of the antenna 402 to tune the transmit and/or receive frequency. In addition, the switch plus tuning circuit 404 may selectively switch the antenna 402 on and off in response to at least a command from the CPU 408. In some implementations, the antenna 402 can be a short range wireless antenna connected to an NFC inlay via a software switch such as an NAND Gate or other element to allow 25 for code from the CPU 408 to turn the antenna 402 on and off. In some implementations, the card 400 may include an NFC inlay (not illustrated) that can be a passive implementation of NFC short range wireless technology deriving power from the reader terminal in order to transmit data back or a stronger implementation using an eNFC chipset to power active reader mode and self-train mode. In addition, the 30 card 400 may include an external needle point reset (not illustrated) that prompts the CPU 408 to depersonalize the memory or secure element.

The CPU 408 may transmit the switching command in response to an event such as a user request, completion of a transaction, and/or others. When switched on,

the security chip and contactless chipset 406 is connected to the antenna 402 and executes one or more of the following: format signals for wireless communication in accordance with one or more formats; decrypt received messages and encrypt transmitted messages; authenticate user credentials locally stored in the memory 410; 5 and/or other processes. The memory 410 may include a secure and non-secured section. In this implementation, the secure memory 410 may store one or more user credentials that are not accessible by the user. In addition, the memory 410 may store offline Web pages, applications, transaction history, and/or other data. In some implementations, the memory 410 may include Flash memory from 64 MB to 32GB.

10 In addition, the memory 410 may be partitioned into user memory and device application memory. The chipset 406 may include a security module that is, for example Visa and/or MasterCard certified for storing financial vehicle data and/or in accordance with global standards. In addition to a user's financial vehicle, the secure element may store signatures of allowed host devices and/or antenna modes.

15 In some implementations, the CPU 408 may switch the antenna 402 between active and inactivate mode based, at least in part, on a personalization parameter defined by, for example, a user, distributor (e.g., financial institution, service provider), and/or others. For example, the CPU 408 may activate the antenna 402 when the intelligent card 400 is physically connected to a host device and when a 20 handshake with the host device is successfully executed. In some implementations, the CPU 408 may automatically deactivate the antenna 402 when the intelligent card 400 is removed from the host device. In some implementations, the antenna 402 is always active such that the intelligent card 400 may be used as a stand-alone access device (e.g., device on a keychain). In regards to the handshaking process, the CPU 25 408 may execute one or more authentication processes prior to activating the intelligent card 400 and/or antenna 402 as illustrated in FIGURE 7. For example, the CPU 408 may execute a physical authentication, a device authentication, and/or a user authentication. For example, the CPU 408 may activate the antenna 402 in response to at least detecting a connection to the physical interface with the host device (e.g., SD 30 interface) and successful installation of the device driver for mass memory access (e.g., SD device driver) on the host device. In some implementations, device authentication may include physical authentication in addition to a signature comparison of a device signature stored in memory (e.g., security module (SE)) that

was created during first-use (provisioning) to a run-time signature calculated using, for example, a unique parameter of the host device. In the event no host device signature exists in the memory, the CPU 408 may bind with the first compatible host device the card 400 is inserted into. A compatible host device may be a device that can 5 successfully accomplish physical authentication successfully. If a host-device signature is present in the memory, the CPU 408 compares the stored signature with the real-time signature of the current host device. If the signatures match, the CPU 408 may proceed to complete the bootstrap operation. If the signatures do not match, host device is rejected, bootstrap is aborted and the card 400 is returned to the mode it was 10 before being inserted into the device.

User authentication may include verification of physical connection with a user using a PIN entered by the user, a x.509 type certificate that is unique to the user and stored on the host device, and/or other processes. Device and user authentication may verify a physical connection with device through comparison of a device signature and 15 user authentication through verification of user PIN or certificate. In some implementations, the user can select a PIN or certificate at provisioning time. If this case, the CPU 408 may instantiate a software plug-in on the host device. For example, a software plug-in may request the user for his PIN in real time, read a user certificate installed on the device (e.g., x.509), and/or others. The operation of the software plug- 20 in may be customized by the provider. Regardless, the returned user data may be compared with user data stored in the memory. In case of a successful match, the antenna 402 may be activated. In case of an unsuccessful match of a certificate, then card 400 is deactivated. In case of unsuccessful PIN match, the user may be requested to repeat PIN attempts until a successful match or the number of attempts exceeds a 25 threshold. The disk provider may customize the attempt threshold.

In regards to network authentication, the host device may be a cellphone such that the card 400 may request network authentication prior to activation. For example, the card 400 may be distributed by a Wireless Network Operator (WNO) that requires a network authentication. In this example, a flag in memory may be set to ON 30 indicating that network authentication is required. If the flag is set to ON, a unique identity about the allowed network is locally stored in memory such a Mobile Network Code for GSM networks, a NID for CDMA networks, a SSID for broadband networks, and/or identifiers. If this flag is ON, the CPU 408 in response to at least insertion may

request a special software plug-in to be downloaded to the host device and instantiated. This software plug-in may query the host device to respond with network details. In some cases, the type of unique network identity employed and the method to deduce it from the host device may be variable and dependent on the network provider and 5 capability of the host device. If the locally-stored ID matches the request ID, the CPU 408 activated the antenna 402 to enable access or otherwise services are denied.

FIGURE 5 illustrates an example transaction system 500 for wirelessly communicating transaction information using one of a plurality of interfaces. For example, the system 500 may interface the transaction card 112 using a wired or 10 wireless interface. In regards to wired interfaces, the system 500 includes an adaptor 504 and a reader 506. The adaptor 504 can include any software, hardware, and/or firmware configured to translated between a format compatible with the card 112 and a format compatible with the client 104c. For example, the adaptor 504 may translate between microSD protocol and a USB protocol. The reader 506 can include any 15 software, hardware, and/or firmware configured to directly interface with the card 112h. For example, the reader 506 may be a microSD reader such that the client 104d interfaces with the card 112h using a microSD protocol. In regards to wireless interfaces, the system 500 may include a cellular interface 502 and a short-range wireless interface 508. In regards to the cellular interface 502, the financial 20 institutions 106 may wirelessly communicate with the transaction card 112e using the cellular radio technology of the mobile device 110e. For example, the cellular interface 502 may be a CDMA interface, a GSM interface, a UMTS interface, and/or other cellular interfaces. In regards to the short-range wireless interface 508, the financial institutions 106 may wirelessly communicate with the transaction card 112f 25 using, for example, WiFi technology. The short-range wireless interface 508 may be an 802.11 interface, a Bluetooth interface, and/or other wireless interface. In these implementations, the client 104e may include a transceiver used for wireless communication with the transaction card 112f.

FIGURE 6 is a schematic diagram 600 of personalization of a intelligent card 30 (e.g., the transaction card 112, the service card 210). In particular, the intelligent card may be personalized prior to being issued to a user, *i.e.*, pre-issuance, or after being issued to a user, *i.e.*, post-issuance. In regards to pre-issuance, intelligent cards may be personalized in mass batches at, for example, a factory. In this example, each

intelligent card may be loaded with user credentials, security framework, applications, offline Web pages, and/or other data. In some implementations, a intelligent card may be personalized individually at, for example, a bank branch. In this case, a intelligent card may be individually loaded with data associated with a user after, for example, 5 purchasing the disk. As for post issuance, the intelligent card may be personalized wirelessly. For example, the transaction card 112 may be personalized through a cellular connection established using the mobile device 110. In some implementations, an intelligent card may be personalized by synchronizing with a computer such as client 104. The transaction card 112 may receive from an enterprise 10 at least associated with the financial institution 106 that personalization data prior to activation including user credentials, payment application and at least one of operational flags, rule table or user interface. The personalization data present in the card may be updated after activation using at least one of the following methods: 15 wireless or over the air messages containing special and secure update instructions; internet or client application running on a PC connected to the transaction card 112 via the host device or a card reader; internet application wirelessly connecting to the transaction card 112 via the host mobile device or user interface application of the transaction card 112 itself; and/or other methods.

In some implementations, provisioning of the intelligent card can be based, at 20 least in part, on the distribution entity (e.g., financial institution, wireless operator, user). For example, the intelligent card may be distributed by a financial institution such as a bank. In the bank implementation, the intelligent card can be pre-provisioned with user accounts. In this case, the intelligent card may be activated in response to at least initial insertion into a host device. The antenna mode may be set to 25 physical authentication only by default. In some examples, the user may self-select a PIN authentication to prevent unauthorized use or through a PC cradle and plug-in management software if the host device does not have a screen and keyboard. In the wireless-operator implementation, the intelligent card may require device authentication before activation. In some examples, the user may provision financial 30 data (e.g., credit or debit) using one of several methods. In addition, the user may add user authentication. In the user-provided implementation, the user may acquire the intelligent card from, for example, a retail store or other channels like OEM host

device manufacturers. In this case, the user may activate the card in a plurality of different devices with provider selected provisioning.

In regards to activating for financial transactions, the intelligent card may be configured in memory mode when user acquires the disk from, for example a bank, a wireless operator, a third-party provider, and/or others. Activation of the card may include the following two levels: 1) physically, specifying antenna availability under a specific set of circumstances desired by the provider; and b) logically, at the financial institution signifying activation of the financial vehicle carried on the card. In some implementations, activation may be based, at least in part on device distributor, antenna availability selection, and/or type of host device as illustrated in Table 1 below.

Table 1:

Plug-in Seller and Mode of distribution	Plug-In Initial State and Antenna Availability Choice	Device Has No Screen /Keyboard	Device Has Screen & keyboard
FI: Financial Institution (bank or retailer) ships plug-in directly to the subscriber or through participating resellers/ distributors etc.	Plug-In is in Memory Mode, It is fully personalized with user's account information (FV) and Antenna mode is set to Physical Authentication	Manual: User has to call FI's number to activate his account, the Device can only work with a single account. User can also access FI's site on the internet using another PC to activate his account	If the device is capable of wireless access, upon insertion, the plug-in spawns a web page and takes the user to FI's website. The user self activates his account by entering his account number and matching secret personal information (last 4 digits of SSN or home phone number for example). The user can also optionally select a PIN (change Antenna availability to user authentication) at the same time. If Internet connection is not available, the device can automatically dial a voice

			call to FI's number for account activation. If wireless connection is not available as well (device is only a PDA), the user has to fallback to manual activation (see left)
WNO: Wireless Network Operator Ships plug-in bundled with host device, User can select his preferred host device and plugin is bundled with it if user would like to avail of this service	Plug-In is in Memory Mode, it is partially personalized (device signature of the host device loaded to prevent user from changing host device) while FV information is not loaded. Antenna Availability is set to Device Authentication (plug-in can only used with host device it is shipped with)	Not Applicable	Assumption: Device has a functional wireless connection. Operator offers a bundled wallet management application. When user clicks the wallet management application, the user is invited to sign-up with operator's partner FI for a new account. Once sign-up is successful, account data is downloaded Over the Air or Over the Internet to the plugin and it is activated for use. Device can use multiple FIs in this scenario and store multiple FVs. User can select to enter a PIN for an FV in the wallet management application in order to convert Antenna availability to user and device authentication for that FV. Plug-in is bound to a device signature. When removed from the device, the Antenna turns off and the plug-in turns into a simple mass memory

			stick. When Plug-in is inserted into another host device, the signature doesn't match and Antenna remains off.
WNO: Wireless Network Operator Ships plug-in as an accessory with an advice for compatible devices, User can select his preferred host device and attempt to operate his plug-in with, to avail of the service	Plug-In is in Memory Mode, it is unpersonalized. Antenna Availability is set to Network authentication is set to On. Plug-In will bind to first device it is inserted in and where network authentication is successful	Not Applicable	Assumption: Device has functional wireless connection. Plug-In will spawn an internet connection to the operator portal and the wallet management application will be downloaded upon user confirmation. User can reject download and choose to manually provision FV data by going to a third party wallet provider or directly to the FI website. Plug-In is bound to the device and to the network provider's network. If the same device is unlocked and used on another network, the plug-in will cease to operate and will revert back to memory mode. When removed from the device, the plug-in will revert to the memory mode.
OEM 1: Cellphone manufacturer	Device Authentication (device comes bundled with a cellphone)	Not Applicable	Option A: Device Manufacturer offers a wallet management application, rest of the process remains as above Option B: Wireless

			<p>Operator offers a wallet management application. User goes to the wireless operator portal and downloads this application Over the Air. The rest of the process then remains the same as above</p> <p>Option C: User navigates to a third party wallet management application (example paypal or Google). Sign up is offered to participating FIs and FVs are personalized on the plug-in Over the Internet</p> <p>Option D: User navigates to FI's website and activates a new account which is personalized over the Internet on the plug-in</p>
OEM 2: Other manufacturer	Device Authentication	<p>User has to cradle the device to the PC with an internet connection and sign-up on the PC by going to an FI's website directly. Account is downloaded over the internet via the cradle and then the device is activated. In this process, the plug-in is bound to the device signature. When removed from the host device, the antenna</p>	<p>If the device has wireless connection (it is a wireless PDA): Same as above</p> <p>If the device has no wireless connection (it is an unconnected PDA): Same as left</p>

		turns off When plugged into another device, the device signature fails and the device behaves like a mass memory device only	
--	--	--	--

The illustrated chart is for example purposes only. The user may activate an intelligent card using the same, some, or different processes without departing from the scope of this disclosure.

5 FIGURE 7 is a flow chart illustrating an example method 700 for automatically bootstrapping an intelligent card in response to at least insertion into a host device. In general, an intelligent card may execute one or more authentication procedures prior to activation. Many of the steps in this flowchart may take place simultaneously and/or in different orders as shown. System 100 or system 200 may use methods with
10 additional steps, fewer steps, and/or different steps, so long as the methods remain appropriate.

Method 700 begins at step 702 where insertion into a host device is detected. For example, the transaction card 112 may detect insertion into the mobile device 110. If authentication is not required for any aspect of the intelligent card at decisional step
15 704, then execution ends. If authentication is required for at least one aspect, then execution proceeds to decisional step 706. If communication with the host device includes one or more errors, then, at step 708, a failure is indicated to the user. In the example, the transaction card 112 may present an indication of a communication error to the user using the GUI 111. If a communication error is not detected at decisional
20 step 706, then execution proceeds to decisional step 710. In some implementations, the intelligent card uploads an SD driver to the host device. If the intelligent card only requires physical authentication, then execution proceeds to decisional step 712. If the network authentication flag is not set to on, then, at step 714, the antenna is turned on and the intelligent card is updated with host-device signature. As for the example, the
25 transaction card 112 may activate the antenna for wireless transactions and update local memory with the host-device signature. If the network authentication flag is turned on at decisional step 712, then, at step 716, the intelligent card transmits a

request for the network ID to the host device. Next, at step 718, the intelligent card retrieves a locally-stored network ID. If the stored network ID and the request network ID match at decisional step 720, then the disk is activated at step 714. If the two network ID's do not match, then the antenna is deactivated at step 722.

5 Returning to decisional step 710, if the authentication is not only physical authentication, then execution proceeds to decisional step 724. If the authentication process includes device authentication, then, at step 726, the intelligent card transmits a request for a network ID to the host device. At step 728, the intelligent card retrieves a locally stored device signatures. If the intelligent card does not include at least one 10 device signature, then execution proceeds to decisional step 734. If the intelligent card includes one or more device signatures, then execution proceeds to decisional step 732. If one of the device signatures matches the request network ID, then execution proceeds to decisional step 734. If the signatures and the request network ID do not match, then execution proceeds to step 722 for deactivation. If user authentication is 15 not included in the authentication process, then execution proceeds to decisional step 712 for physical authentication. If user authentication is included at decisional step 734, then execution proceeds to step 738.

 Returning to decisional step 724, if the authentication process does not include device authentication, then execution proceeds to decisional step 736. If user 20 authentication is not included in the process, then, at step 722, the intelligent card is turned off. If user authentication is included, then, at step 738, the intelligent card request a PIN number from the user using the host device. While the user authentication is described with respect to entering a PIN through the mobile host device, the user may be authenticated using other information such as biometric 25 information (e.g., fingerprint). Again returning to the example, the transaction card 112 may present a request for the user to enter a PIN through the GUI 111. At step 740, the intelligent card retrieves a locally-stored PIN. If the request PIN and stored PIN match at decisional step 742, then execution proceeds to decisional step 712 for physical authentication. If the request PIN and the stored PIN do not match at 30 decisional step 742, then execution proceeds to decisional step 744. If the number of attempts have not exceeded a specified threshold, then execution returns to step 738. If the number of attempts has exceed to the threshold, then the antenna is deactivated at step 722. In the example, if the event that the transaction card 112 fails to authorize

the device, network and/or user, the transaction card 112 may wirelessly transmit an indication to the associated financial institution using the cellular radio technology of the mobile host device 110. In this case, the illustrated method 700 may be implemented as a fraud control process to substantially prevent unauthorized use of the 5 transaction card 112.

FIGURE 8 is an example call flow 800 in accordance with some implementations of the present disclosure. As illustrated, the flow 800 includes a network 802, a host device 804, an intelligent card 806, and a terminal 808. The host device 804 is configured to communicate with the network 802 and includes a slot for 10 insertion of the intelligent card 806. The intelligent card 806 is configured to transmit commands to and receive data from a user interface application 810 executed by the host device 810 and execute transactions independent of the host device 810. The card 806 includes a CPU 812 for executing transactions and a wireless chipset 814 for communicating with the terminal 808. The CPU 812 executes a host controller/API 15 interface 816 configured to transmit commands in a form compatible with the host device 804 and convert data from the host device 804 to a form compatible with the CPU 812.

As illustrated, the flow 800 may include multiple sessions 820 between the host device 804 and the card 806 and between the card 806 and the terminal 808. The 20 session 820a illustrates a session managed by the card 806 using the network capabilities of the host device 810. In this example, the card 806 transmits data for transmission through a cellular network connected to the host device 804, and after receiving the cellular data, the host device 804 transmits the data to the network 802. In response to receiving data from the network 802, the host device 804 may 25 automatically transmit the received data to the card 806. In some implementations, the card 806 may transmit a request for a device signature to the host device 804 as illustrated in session 820b. For example, the card 806 may request the device signature during a bootstrapping process. The session 820c illustrates that a user may submit commands to the card 806 through the interface of the host device 804. For 30 example, the user may request that the disk display the user's transaction history through the interface of the host device 804.

In some implementations, the card 806 may receive a command to activate or deactivate the antenna through the host device 804 as illustrated in session 820d. For

example, a financial institution may identify irregular transactions and transmit a command through the network 802 to deactivate the card 806. The card 806 may authorize a user by requesting a PIN using the host device 804. As illustrated in session 820e, the user may submit a PIN to the card 806 using the interface of the host 5 device 804, and in response to an evaluation of the submitted PIN, the card 806 may present through the host device 804 an indication that the user verification is successful or has failed. In some implementations, a user and/or financial institution may request a transaction history of the card 806 as illustrated in session 820f. For example, a financial institution may transmit a request for the transaction history 10 through the network 802 connected to the host device 804, and in response to at last in the request, the card 806 may transmit the transaction history to the financial institution using the network 802 connected to the host device 804. In some implementations, the user may present offline Web pages stored in the card 806 as illustrated in session 820. For example, the card 806 may receive a request to present 15 an offline Web page from the user using the host device 804 and present the offline page using the URL in the request. In some implementations, data stored in the memory of the card 806 may be presented through, for example, the host device 804 as illustrated in session 820h. For example, the user may request specific information associated with a transaction on a certain data and the card 806 may retrieve the data 20 and present the data to the user using the host device 804. In addition, the user may write data to the memory in the card 806 as illustrated in session 820i. For example, the user may update transaction data with an annotation, and in response to at least the request, the card 806 may indicate whether the update was a success or failure.

In regards to session between the card 806 and the terminal, the flow 800 25 illustrates the personalization session 820k and the transaction session 820l. In regards to personalization, a financial institution may personalize a card 806 with user credentials, user applications, Web pages, and/or other information as illustrated in session 820k. For example, the terminal 808 may transmit a provisioning request to the card 806 including associated data. The protocol translation 818 may translate the 30 personalization request to a form compatible with the card 806. In response to at least the request, the CPU 812 transmit an indication whether the personalization was a success or not using the protocol translation 818. Prior to the terminal executing a transaction, the terminal 808 may submit a transaction challenge to the card 806 as

illustrated in session 8201. In this case, the card 806 may identify a device signature of the host device 804, present associated data to the user through the host device 804, and transmit the signature to the terminal 808 using the protocol translation 818.

FIGURE 9 is a flow chart illustrating an example method 900 for activating a wireless transaction system including an intelligent card. In general, an intelligent card may execute one or more activation processes in response to, for example, a selection from a user. Many of the steps in this flowchart may take place simultaneously and/or in different orders as shown. System 100 or system 200 may use methods with additional steps, fewer steps, and/or different steps, so long as the methods remain appropriate.

Method 900 begins at step 902 where a request to activate a transaction card is received. For example, the user may select a graphical element displayed through the GUI 111 of a mobile host device 110 in FIGURE 1. If an account activation is included at decisional step 904, then at step 906, a request to activate the associated financial account is wirelessly transmitted to financial institution using cellular radio technology of the host device. For example, the transaction card 112d of FIGURE 2 may wireless transmit an activation request to the financial institution 106 using the cellular radio technology of the mobile host device 110d. If an account activation is not included, then execution proceeds to decisional step 908. If card activation is not included, then execution ends. If card activation is included, then execution proceeds to decisional step 910. If an activation code is not included, then at step 912, one or more preprogrammed questions are presented to the user using the GUI of the host device. Returning to the initial example, the transaction card 112 may identify locally stored questions and present the questions to the user using the GUI 111 of the mobile host device 110. At step 914, locally-stored answers to the programmed questions are identified. Returning to decisional step 910, if an activation code is included, then execution proceeds to decisional step 916. If the activation code is manually entered by the user, then at step 918, a request for the activation code is presented to the user through the GUI of the mobile host device. In the initial example, the transaction card 112 may present a request for an activation code such as a string of characters to the user through the GUI 111 of the mobile host device 110. If the activation code is not manually entered by the user, then at step 920, the transaction card wirelessly transmits a request for the activation code using the cellular radio technology of the host device.

In the cellular example, the transaction card 112 may transmit a request to the financial institution using the cellular core network 202. In either case, the locally-stored activation code is identified at step 922. If the locally stored information matches the provided information at decisional step 924, then at step 926, the transaction card is activated. For example, the transaction card 112 may activate in response to at least a user entering a matching activation code through the GUI 111. If the provided information does not match the locally stored information, then execution ends.

FIGURES 10A and 10B illustrate example cards 1000 and 1020, respectively, for housing the transaction card 112 of FIGURE 1. For example, the transaction cards 112 may be inserted into the cards 1000 and 1020 during the personalization process and/or distribution processes. By executing personalization while inserted, the transaction cards 112 may be personalized using the same systems used to personalize smart cards with substantially no alterations. In other words, the cards 1000 and 1020 may have substantially similar dimensions as smart cards such that personalization systems may similarly process the cards 1000 and/or the 1020. In FIGURE 10A, the card 1000 includes a slot 1002 formed to hold the transaction card 112. For example, the slot 1002 may retain the transaction card using a frictional fit such as internal serrations. When retained in the slot 1002, the transaction card 112 may be substantially flush with the front and back surfaces of the card 1000. In FIGURE 10B, the card 1020 includes a pocket 1022 for retaining the transaction card 112 at least adjacent a surface of the card 1020. In some implementations, the cards 1000 and 1020 may include magnetic strips to execute contact transactions.

A number of embodiments of the invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. Accordingly, other embodiments are within the scope of the following claims.

WHAT IS CLAIMED IS:

1. A card, comprising:
 - a physical interface that interfaces the card with a mobile host device including a Graphical User Interface (GUI), wherein the card executes wireless financial transactions independent of the mobile host device;
 - 5 an antenna that wirelessly receives Radio Frequency (RF) signals from and transmits RF signals to retail terminals;
 - secure memory that stores user credentials used to execute the financial transactions with the retail terminals;
 - 10 a user-interface module that presents and receives information through the GUI of the mobile host device; and
 - an antenna control module that selectively switches the antenna between an activate state and an inactive state in response to at least an event.
- 15 2. The card of claim 1, wherein the physical interface comprises at least one of a SecureDigital (SD) interface, a miniSD interface, a microSD interface, , a MMC interface, a miniMMC, a microMMC, a firewire or a apple iDock interface, or a Universal Serial Bus (USB) interface.
- 20 3. The card of claim 1, further comprising a transaction module that identifies the user credentials in the memory and executes wireless transactions with retail terminals as the antenna is in the activated state.
- 25 4. The card of claim 1, further comprising a Central Processing Unit (CPU) that identifies one or more rules associated with operational aspects of the card and automatically transmits a command to the antenna control function module to deactivate the antenna in response to at least a violation of the one or more rules.
- 30 5. The card of claim 4, wherein the one or more rules are based, at least in part, on identifying at least one of a network, a mobile host device, or a user.

6. The card of claim 4, wherein the one or more rules are based, at least in part, on a change in at least one of a phone number, a MAC address, or a location.

7. The card of claim 4, wherein the CPU automatically updates the one or 5 more rules in response to at least a command received from the mobile host device.

8. The card of claim 4, wherein the one or more rules deactivates the antenna in response to at least removal of the card from the mobile host device.

10 9. The card of claim 4, the CPU further wirelessly transmits a notification to a financial institution indicating a violation of the one or more rules using cellular radio technology of the mobile host device.

15 10. The card of claim 9, wherein the cellular radio technology includes one of Global System for Mobile Communication (GSM), Code Division Multiple Access (CDMA), Universal Mobile Telecommunications System (UMTS), or Worldwide Interoperability for Microwave Access (WiMAX).

11. The card of claim 1, further comprising an authentication module that 20 authenticates at least one of a network of the mobile host device, the mobile host device, or a user.

12. The card of claim 11, wherein the antenna module deactivates the antenna in response to at least a failure to authenticate the at least one of the network 25 of the mobile host device, the mobile host device, or the user.

13. The card of claim 1, further comprising an activation module that activates the card and transmits to the financial institution a request to activate an associated user account in response to at least a user request or an initial insertion into 30 the mobile host device.

14. The card of claim 13, wherein the card is activated based, at least in part, on a user manually entering an activation code through the GUI of the mobile host device.

5 15. A method, comprising:

physically interfacing a card with a mobile host device including a Graphical User Interface (GUI), wherein the card executes wireless financial transactions independent of the mobile host device;

10 storing user credentials used to execute financial transactions with retail terminals;

presenting information through the GUI of the mobile host device; and

selectively switching an antenna of the card between an activate state and an inactive state in response to at least an event.

15 16. The method of claim 15, wherein the physical interface comprises at least one of a SD interface, a miniSD interface, a microSD interface, a MMC interface, a miniMMC, a microMMC, a firewire or a apple iDock interface, or a Universal Serial Bus (USB) interface.

20 17. The method of claim 15, further comprising:

identifying the user credentials; and

executing wireless transactions with retail terminals as the antenna is in the activated state.

25 18. The method of claim 15, further comprising:

identifying one or more rules associated with operational aspects of the card;

and

automatically deactivating the antenna in response to at least a violation of the one or more rules.

30

19. The method of claim 18, wherein the one or more rules are based, at least in part, on identifying at least one of a network, a mobile host device, or a user.

20. The method of claim 18, wherein the one or more rules are based, at least in part, on a change in at least one of a phone number, a MAC address, or a location.

6 21. The method of claim 18, further comprising automatically updating the one or more rules in response to at least a command received from the mobile host device.

10 22. The method of claim 18, wherein the one or more rules deactivates the antenna in response to at least removal of the card from the mobile host device.

15 23. The method of claim 18, further comprising wirelessly transmitting a notification to a financial institution indicating a violation of the one or more rules using cellular radio technology of the mobile host device.

24. The method of claim 23, wherein the cellular radio technology includes one of GSM, CDMA, UMTS, or WiMAX.

25. The method of claim 15, further comprising authenticating at least one of a network of the mobile host device, the mobile host device, or a user.

26. The method of claim 25, further comprising deactivating the antenna in response to at least a failure to authenticate the at least one of the network of the mobile host device, the mobile host device, or the user.

25 27. The method of claim 15, further comprising:
activating the card; and
transmitting to the financial institution a request to activate an associated user account in response to at least a user request or an initial insertion into the mobile host device.

30 28. The method of claim 15, activating the card based, at least in part, on a user manually entering an activation code through the GUI of the mobile host device.

1/11

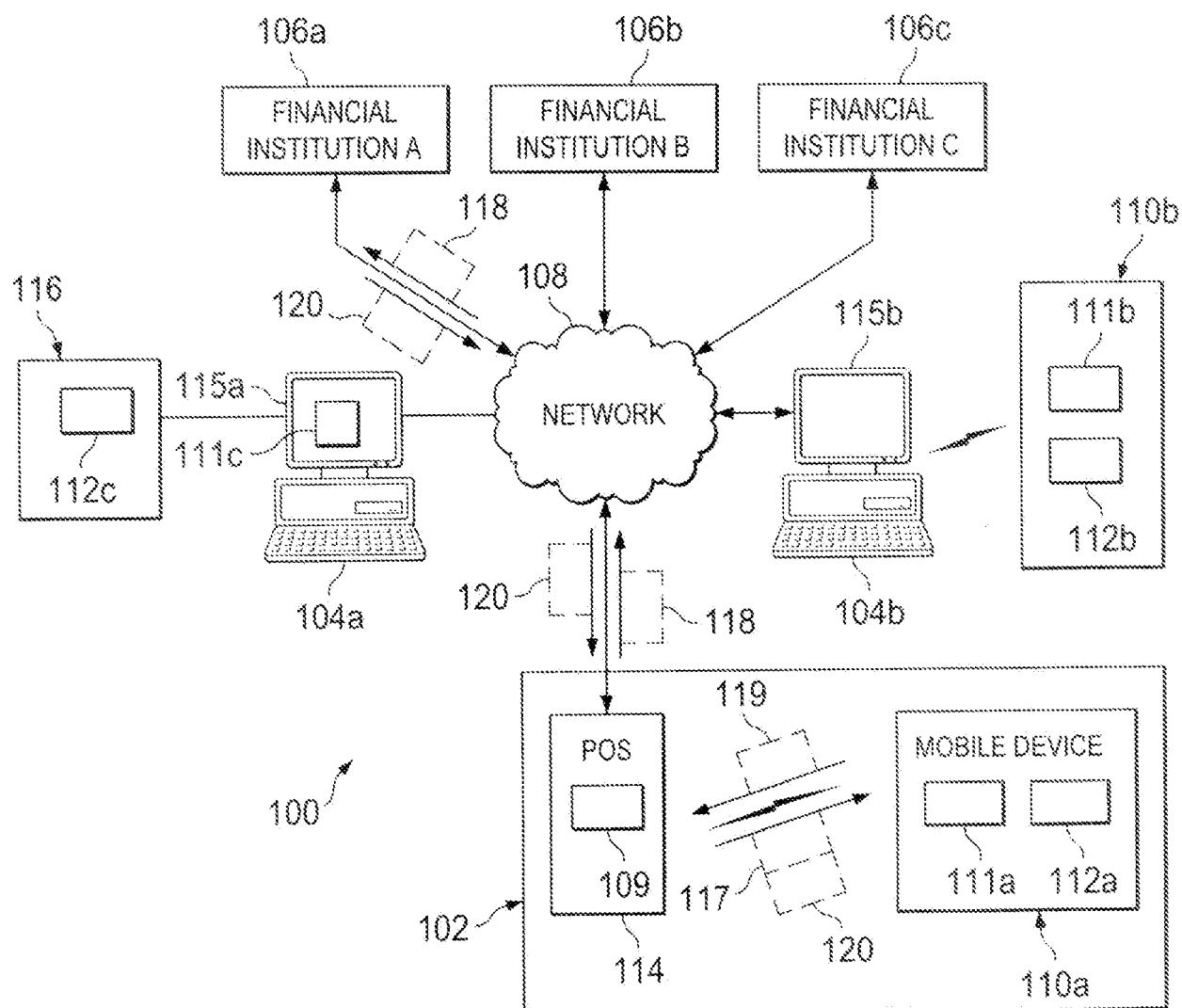


FIG. 1

2/11

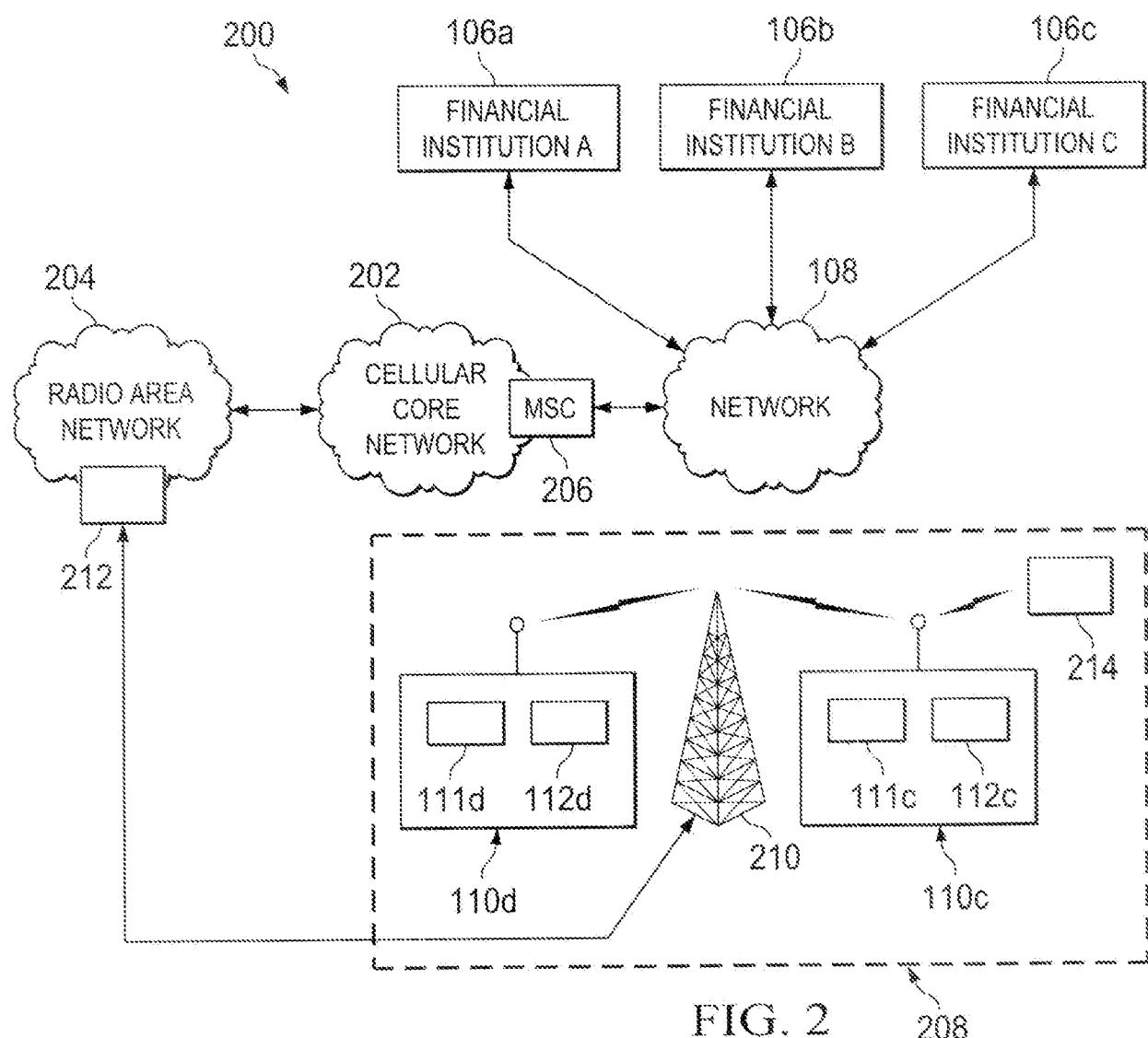


FIG. 2 208

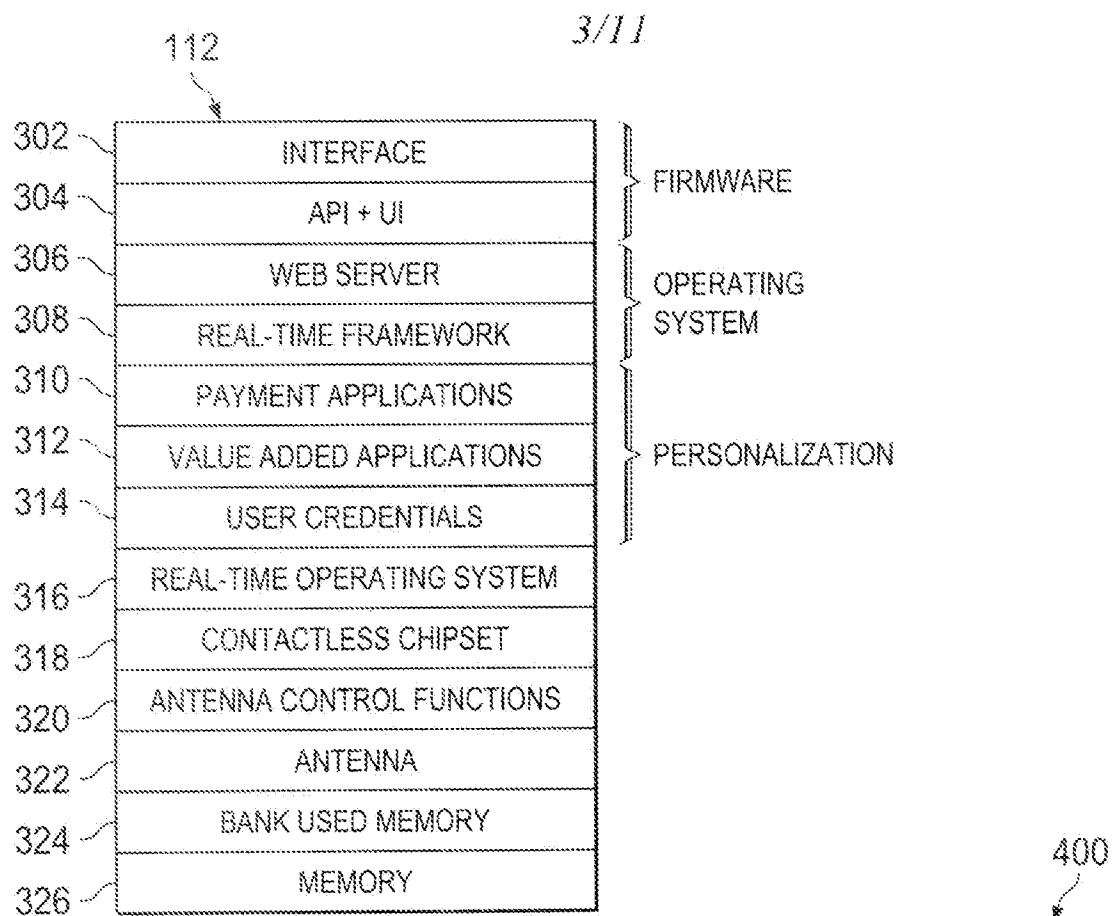


FIG. 3

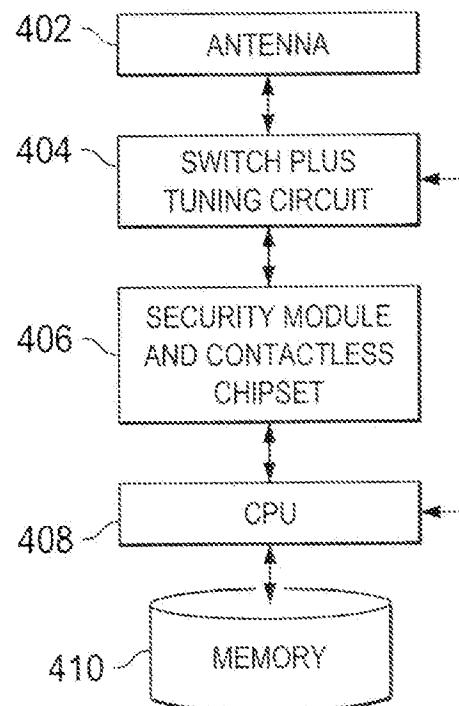
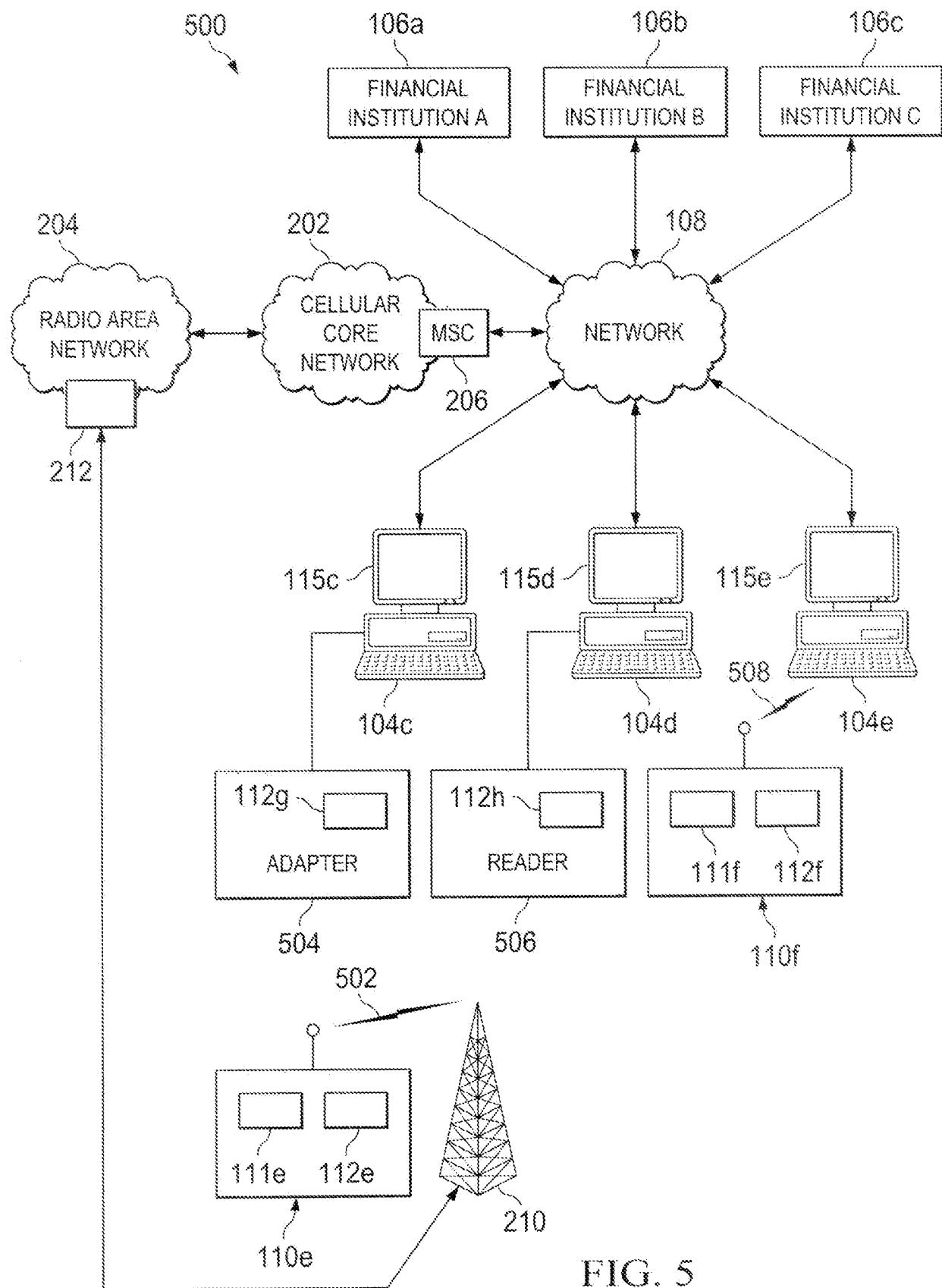


FIG. 4

4/11



5/11

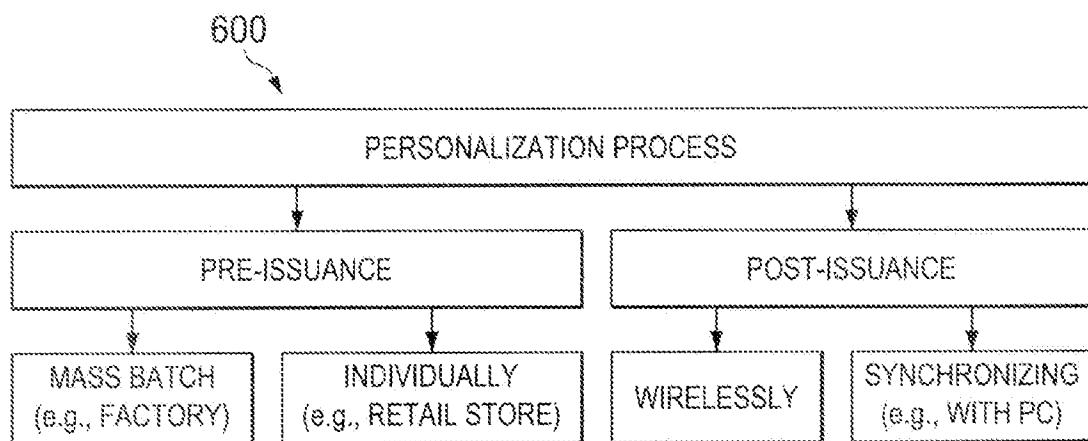


FIG. 6

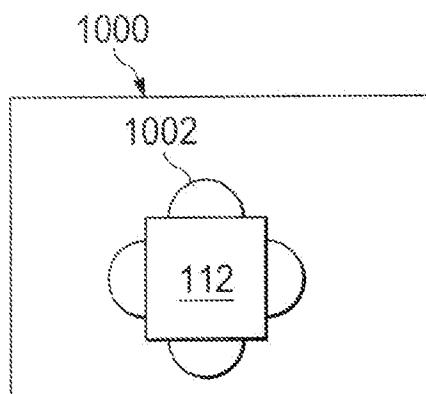


FIG. 10A

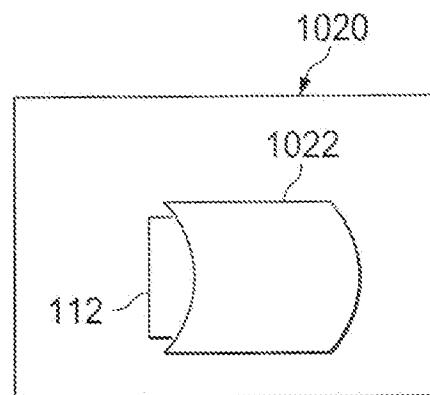


FIG. 10B

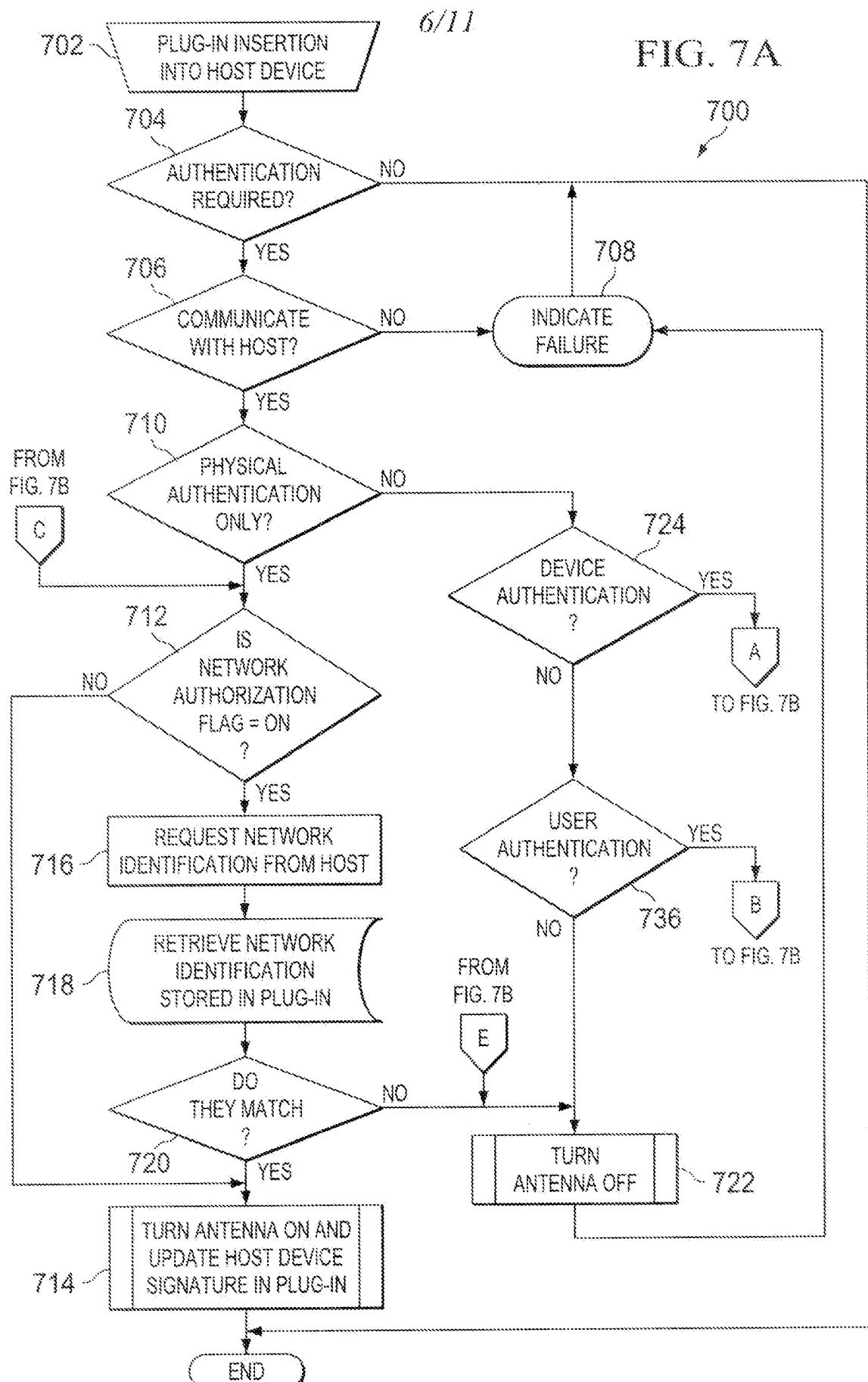
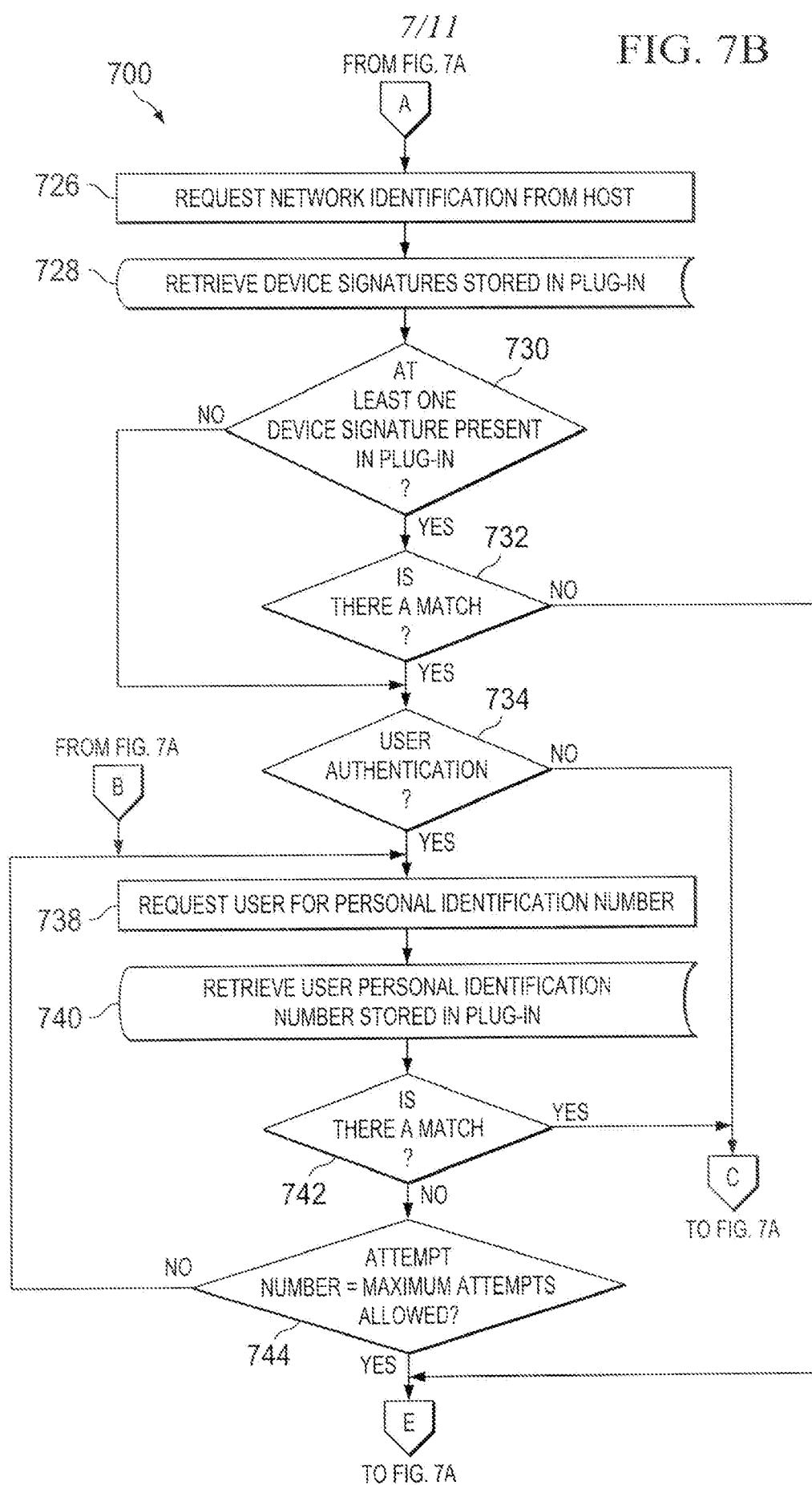


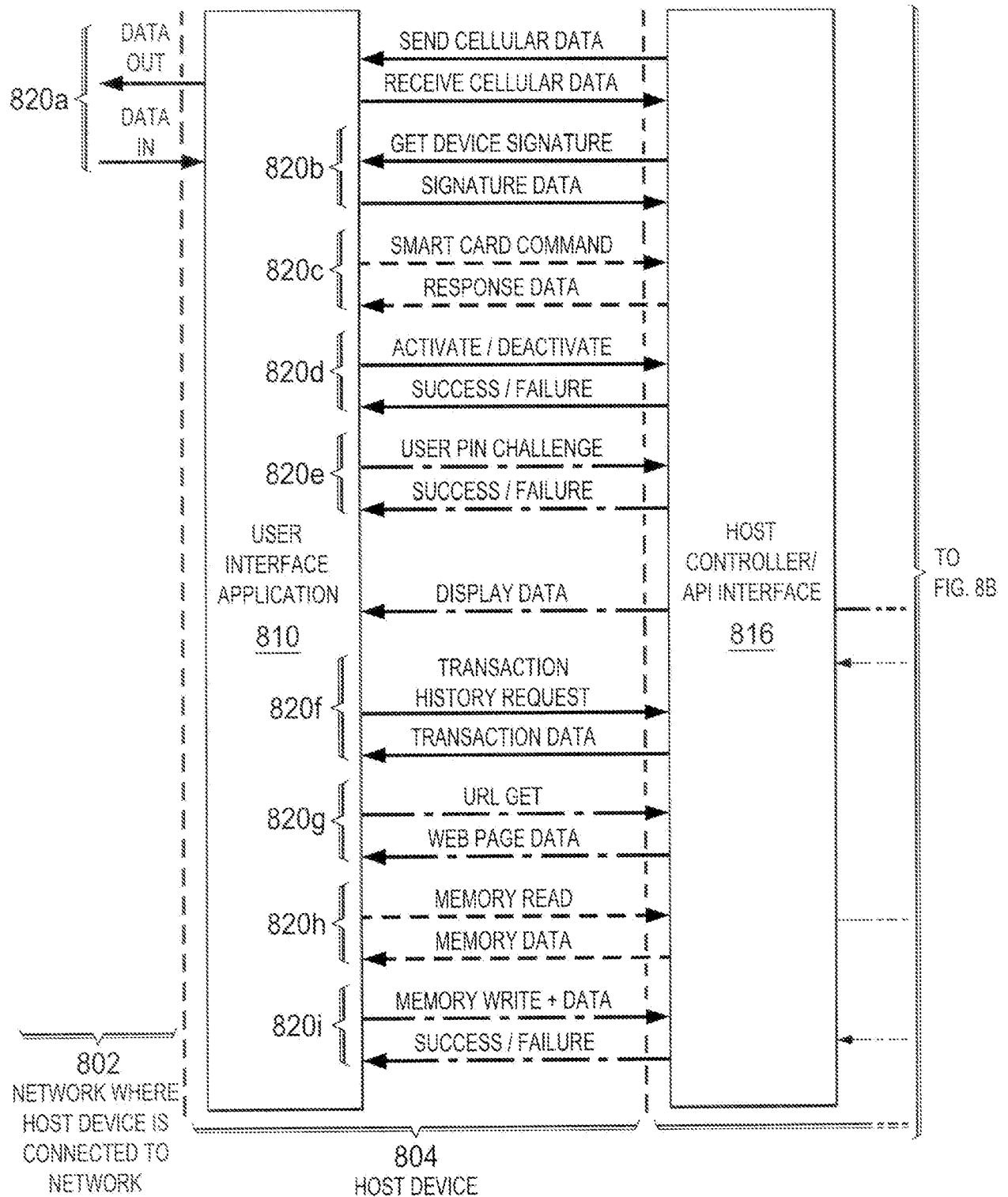
FIG. 7B



8/11

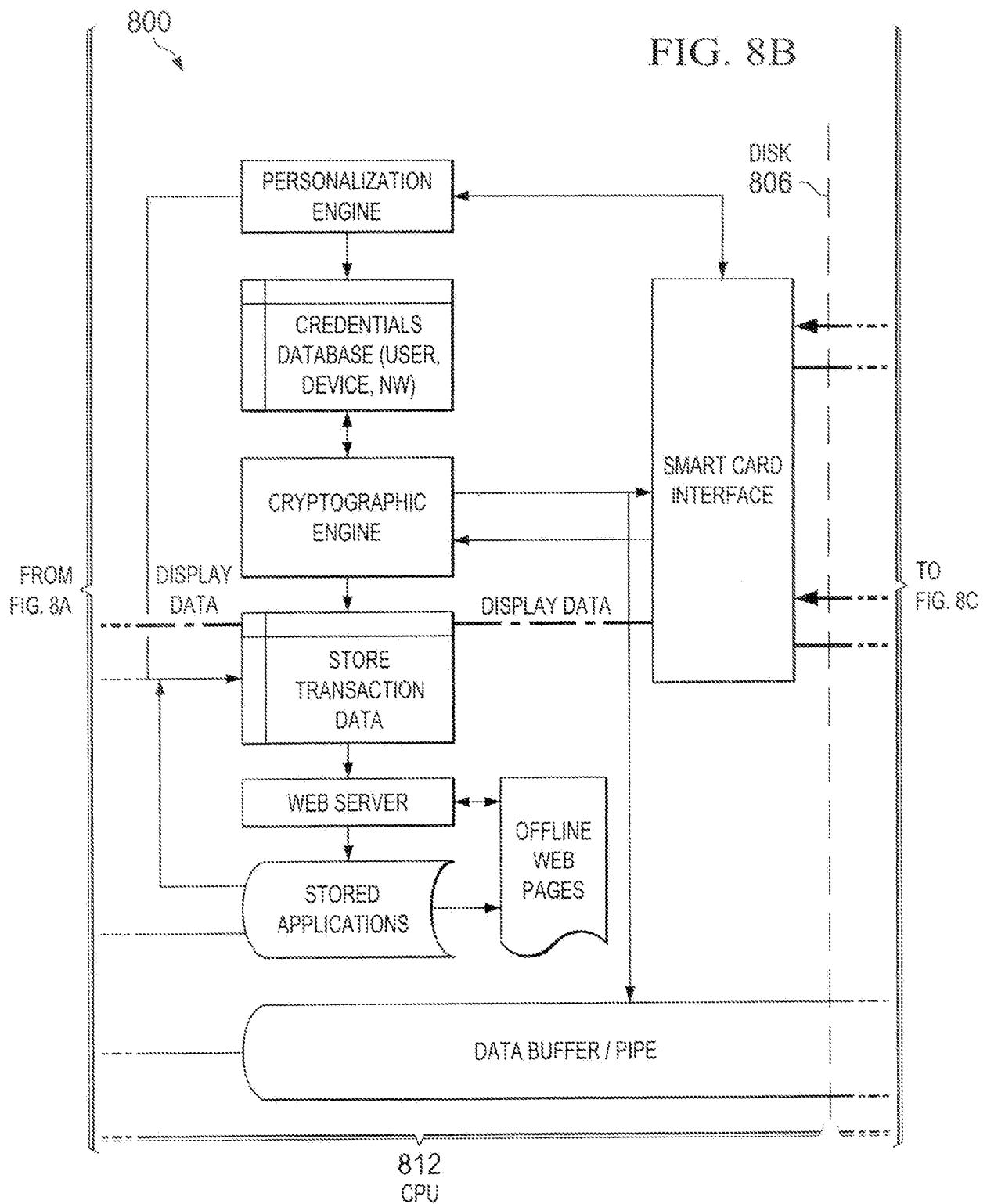
800

FIG. 8A

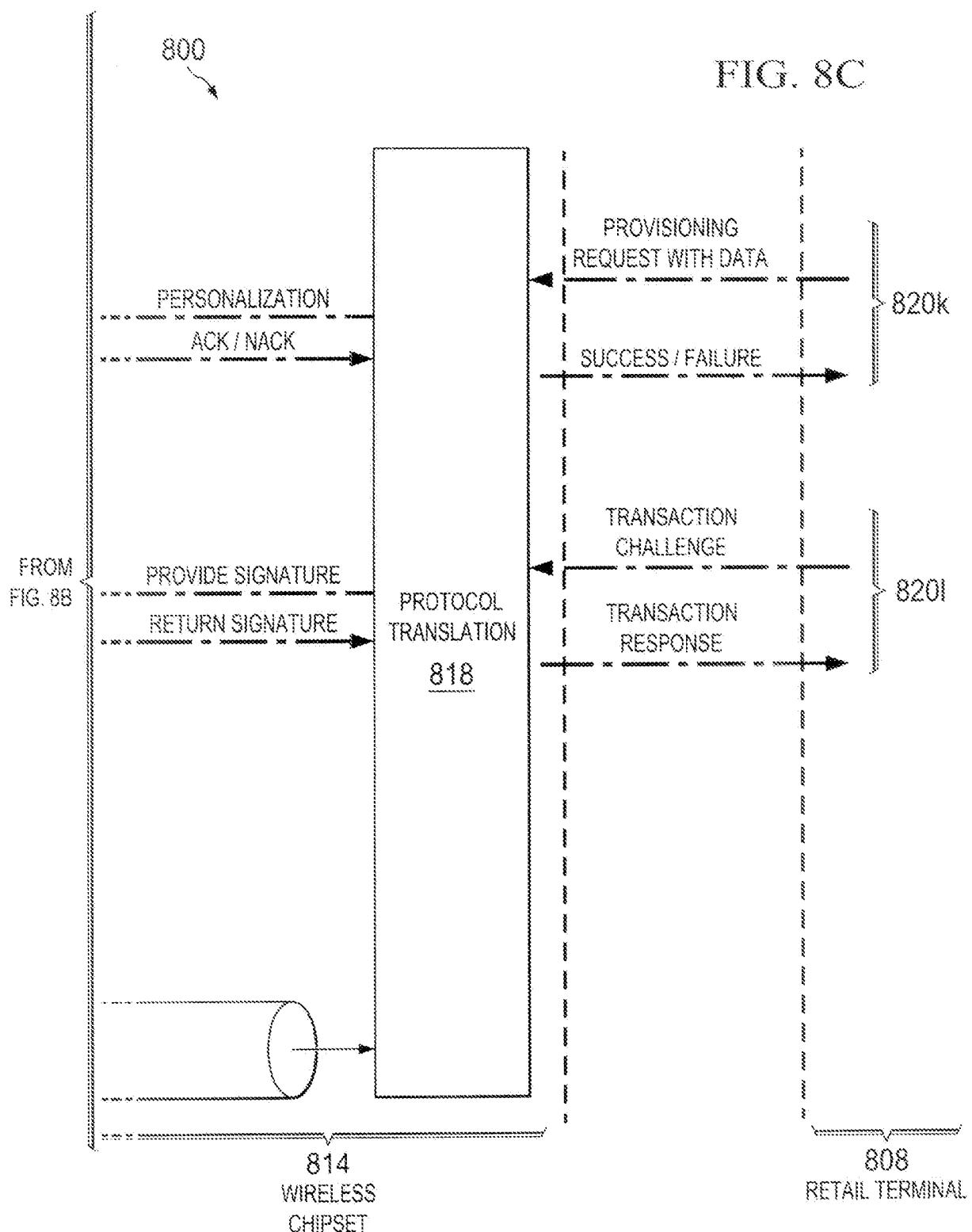


9/11

FIG. 8B



10/11



11/11

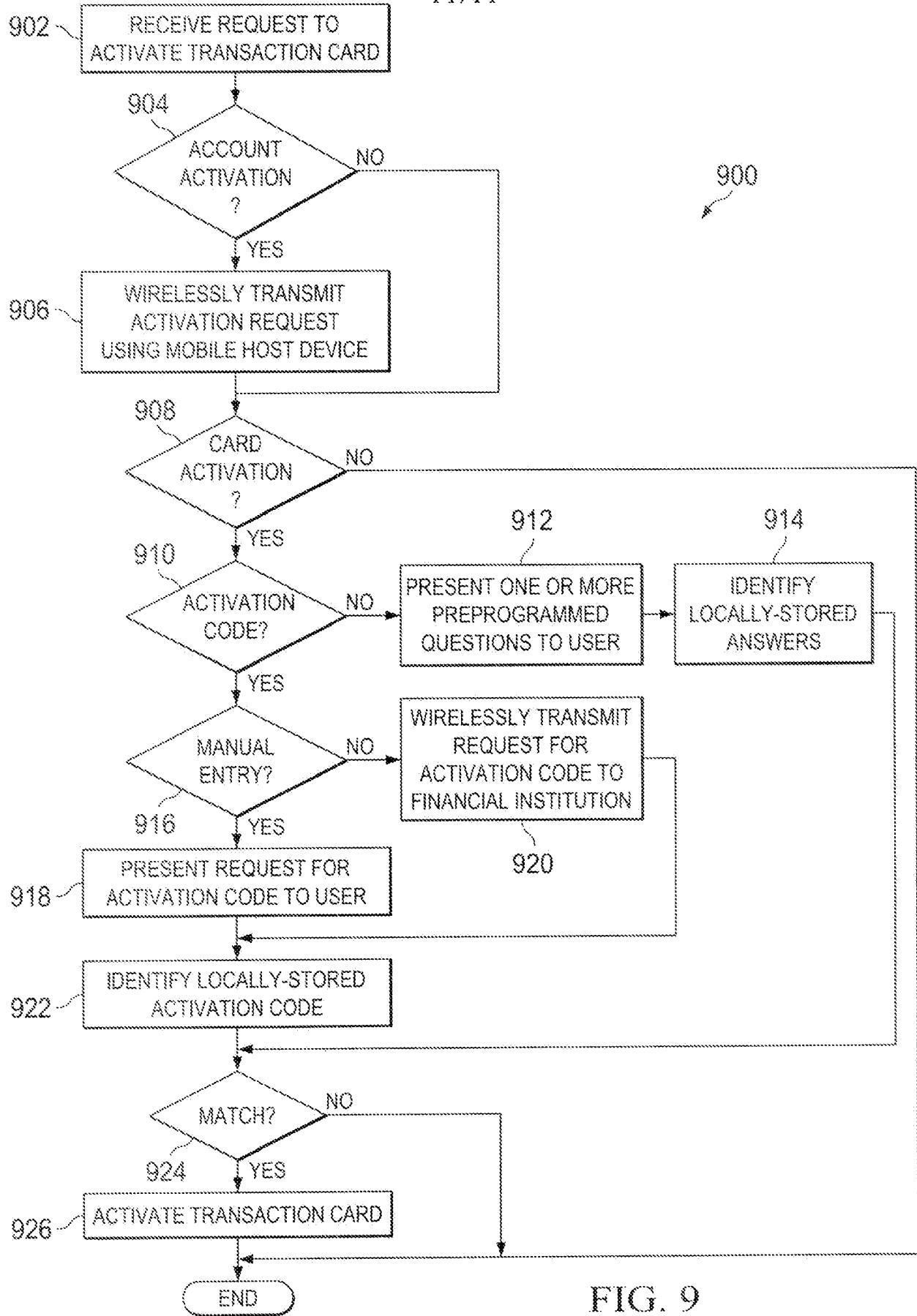


FIG. 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2008/076033

A. CLASSIFICATION OF SUBJECT MATTER

A. CLASSIFICATION OF SUBJECT MATTER
INV. G07F7/10 G06K19/00 H04L29/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system, followed by classification symbols)
G06Q H01Q G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2007/145135 A1 (JOGAND-COULOMB FABRICE [US] ET AL) 28 June 2007 (2007-06-28) paragraphs [0047], [0049], [0058], [0064], [0065], [0071] -----	1-28
Y	WO 2007/088898 A (ORIENT INSTR COMP CO LTD [JP]; ITO TOMOAKI [JP]) 9 August 2007 (2007-08-09) abstract -----	1-28

□ Further documents are listed in the continuation of Box C.

See patent family annex

* Special categories of cited documents :

- **A** document defining the general state of the art which is not considered to be of particular relevance
- **E** earlier document but published on or after the international filing date
- **L** document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- **O** document referring to an oral disclosure, use, exhibition or other means
- **P** document published prior to the international filing date but later than the priority date claimed

- *T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *& document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 December 2008	05/01/2009
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Authorized officer Wolles, Bart

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2008/076033

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007145135 A1	28-06-2007	NONE	
WO 2007088898 A	09-08-2007	NONE	